جريمة الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات وفق التشريع الأردني /دراسة مقارنة

إعداد
محمد سليمان الخوالدة

المشرف
الدكتور احمد موسى هياجنة

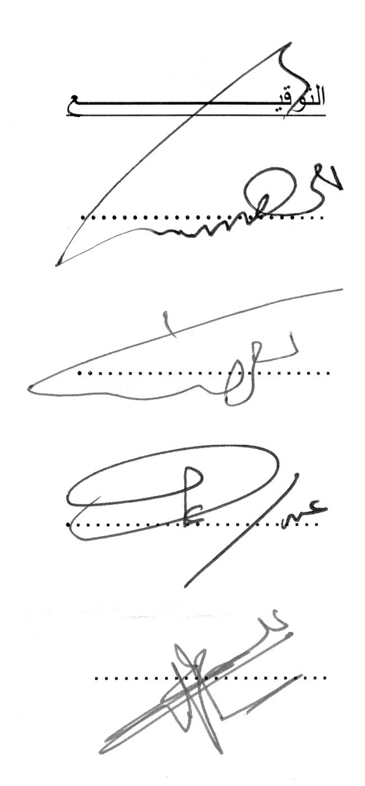
قدمت هذه الرسالة استكمالا لمتطلبات منح درجة الماجستير في القانون العام

كلية الدراسات العليا
الجامعة الأردنية

كانون الثاني ، 2012

نوقشت هذه الرسالة/الأطروحة (جريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات وفق التشريع الاردني /دراسة مقارنة) وأجيزت بتاريخ ٢٠١٢/١/٤

أعضاء لجنة المناقشة	التوقيع
الدكتور أحمد موسى هياجنة ، مشرفاً أستاذ مساعد – قانون جنائي	....
الدكتور نظام توفيق المجالي ، عضواً أستاذ – قانون جنائي	....
الدكتور عبد الإله محمد النوايسة ، عضواً أستاذ – قانون الجنائي (جامعة مؤته)	....
الدكتور سامي حمدان الرواشده أستاذ مشارك – قانون الجنائي	....



الإهـــــــــــداء

إلى والدَيّ أطال الله في عمرهما على طاعته ومتعهما بالصحة والعافية ، إلى زوجتي

أم رعد ، وأبنائي رعد ، راكان ، سليمان ، ريّان ، وزملائي في العمل الذين عانوا

الكثير لأجل إتمامي هذا العمل ، اهدي هذا الجهد المتواضع.

الباحث

شـــكــــــر وتقديـــــر

الحمد الله رب العالمين والصلاة والسلام على أشرف الخلق والمرسلين سيدنا محمد صلى الله عليه وسلم.

اشكر الله سبحانه وتعالى على ما منّ به عليّ من نعم لا تعد ولا تحصى ، ثم الشكر والتقدير للدكتور أحمد موسى هياجنة ، المشرف على هذه الرسالة الذي تعلمت منه الكثير ، والذي لم يدخر جهدا في سبيل مساعدتي لانجاز هذا العمل ، حيث منحني الكثير من وقته وكان لتوجيهاته الأثر الكبير في إعداد هذه الرسالة في صيغتها النهائية فشكرا له على ما قدم وأجزل.

الفهـــــرس

الموضوع **الصفحة**

جريمة الدخول غير المشروع لموقع الكتروني او نظام معلومات وفق التشريع الاردني /دراسة مقارنة

إعداد
محمد سليمان عقله الخوالده

المشرف
الدكتور أحمد موسى هياجنة

ملخـــــــــــص

تتناول الدراسة جريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات وفق التشريع الأردني وتحديدا وفق النصوص الواردة في قانون جرائم أنظمة المعلومات لعام٢٠١٠ ، حيث انتشرت جرائم اختراق المواقع الالكترونية والدخول غير المصرّح به لنظام المعلومات بهدف الاستيلاء على المعلومات أو إتلافها عبر تقنية الفيروسات وغيرها من وسائل التدمير المعلوماتي، وفي هذه الدراسة تناولنا الطبيعة القانونية لجريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات، واهم خصائصها لتطبيقها على واقع النص القانوني من خلال وصف أركان هذه الجريمة وصور النشاط الجرمي المكون لها ،ومسؤولية مرتكب هذا النوع من الجرائم المستحدثة والجزاء المقرر لها وفق نص القانون الأردني مقارنة مع التشريعات الجنائية المقارنة.

وقد خلصت الدراسة إلى عدد من النتائج والتوصيات تمثلت في أن جريمة الدخول غير المشروع لنظام المعلومات أو موقع الكتروني جريمة تعتمد على الذكاء دون أدنى مجهود عضلي، ومن الضروري إدخال نصوص قانونية تعاقب على جريمة إتلاف المعلومات والبيانات بحد ذاتها وتقرر مسؤولية الشخص المعنوي كالشركات والهيئات في حال ارتكاب احد موظفيها إحدى الجرائم المعلوماتية والمعاقبة على الشروع في مثل هذه الجرائم .

مقدمـــــة

ارتبطت الجريمة بالإنسان منذ بداية الخلق على سطح اليابسة ، ولان الإنسان بطبعه كائن اجتماعي ارتبط بالمجتمع ارتباطا فاعلا ومنفعلا ، وبما أن الصلة وطيدة بين الجريمة والمجتمع فان تطور المجتمع الحضاري والعلمي والتكنولوجي انعكس أثره على تطور الجريمة[١]، فالجريمة باعتبارها إحدى صور إفرازات المجتمع يصلها ما يصل المجتمع من تطور، ومرجع ذلك أن مرتكب الجريمة وضحيتها عضوان في المجتمع ويتأثران بحياته وثقافته وتطوره، ونتيجة لهذه الثقافة فإن المجرم يحاول استخدام كل ما لديه من براعة ودراية في ارتكاب جريمته ،فالجريمة هي محصلة لكل تلك المؤثرات.

وقد شهد العالم ثورة من نوع غير مألوف اصطلح على تسميتها بثورة المعلومات،باعتبارها الثورة التي تلت الثورة الصناعية[٢]، فالثورة المعلوماتية الهائلة التي اخترقت الفضاء والمكان بسرعتها المذهلة لتنقل المعلومة (الاتصال بالصوت والصورة) خلال جزء من الثانية لاتمنعها حواجز طبيعية كانت أم سياسية .

وقد أصبحت المعلومة السلعة الرئيسية في العالم كله، أي إن الدول لن تقاس بجيوشها أو قواتها أو ثرواتها ولكن سيكون المقياس الأول لقوة الدولة هو مقدار ما تنتجه في حقل صناعة المعلومات واستخدامها والتعامل معها ،فالمعلومة قوة ، وهذا الانفجار المعلوماتي الذي نشهده الآن هو ثمرة المزواجة بين تكنولوجيا الاتصالات وتكنولوجيا الحاسب الآلي والذي أدى إلى ميلاد علم جديد هو علم الاتصال المعلوماتي (Computer Telecommunications).[٣]

وعلى الرغم من تعدد الإمكانات التي تتيحها شبكة الإنترنت في مجالات المعرفة المتنوعة إلا أن هذه الشبكة قد فتحت الباب واسعًا أمام كثير من المجرمين ليرتكبوا جرائمهم المبتكرة على

---

[١] محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية للنشر والتوزيع - القاهرة ، ١٩٩٨ ، الطبعة الثانية ص ٣

[٢] وليد عاكم ، التحقيق في جرائم الحاسوب ، بحث منشور على الانترنت http://www.wasmia.com/jazy/crime09.pdf ٢٠١١/١٠/١٥

[3] وليد الكشباطي ، جريمة اختراق الانظمة المعلوماتيه ، بحث منشور على http://www.chawkitabib.info/spip.php?article477 ٢٠١١-١١-٩

المستوى المحلي أو على المستوى الدولي [٤]، فانتشر نوع جديد من الجريمة وهو الجريمة الالكترونية.

هناك الكثير من المصطلحات العربية تستخدم للتعبير عن الجرائم المعلوماتية مثل:"جرائم تقنية المعلومات"High-Tech Crime" ، و"الجرائم الالكترونية" "E -Crime" والحاسبات احد عناصرها، وهنالك من يطلق مصطلح "جرائم الحاسب" "Computer Crime" لتشمل معه شبكة الانترنت[٥]، وكذلك تسمى في بعض الأدبيات "جرائم المعلوماتية" " Informatics' Crime" أو "الجرائم الرقمية" "Digital Crime" ، وأخيرا أصبحت تسمى "الجرائم السيبيرية Cyber Crime"،و على الرغم من كثرة هذه المصطلحات يمكن القول بأن الجريمة هي ذاتها، ففي نطاق القانون الجنائي – الذي يطلق عليه أيضا تسميات قانون الجزاء وقانون العقوبات– يمكن تعريف الجريمة بأنها: "فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا"[٦]. أو "عمل أو امتناع عن عمل يرتب القانون على ارتكابه عقوبة"[٧].

وقد شاعت في السنوات الأخيرة طائفة جديدة من الجرائم المعلوماتية التي تستهدف المعلومات وبرامج الحاسب، كالدخول غير المصرّح به إلى أنظمة الحاسوب والشبكات والاستيلاء على المعلومات أو إتلافها عبر تقنية الفيروسات وغيرها من وسائل التدمير المعلوماتي، ومن هنا تتجلى أهمية اختيارنا موضوع " جريمة الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات " رغم ما يكتنف هذا الموضوع من صعوبات جمة ترجع إلى ندرة التطبيقات القضائية وما يتسم به من صبغة علمية بحتة غريبة في تصورنا على بعض رجال القانون.

أهمية الدراسة و أسباب اختيارها

استخدام تقنية المعلومات بشكل كبير والانتشار الواسع لها سيما أجهزة الحاسوب وشبكة الانترنت في الآونة الأخيرة في جميع دول العالم ، ومنها الدول العربية صاحبه ظهور العديد من السلبيات، منها جريمة اختراق المواقع الالكترونية والنظام المعلوماتي . وحيث أن القوانين تعتبر الضمانة لحماية المصالح القانونية وبقدر ما تكون القوانين متطورة بقدر ما تحقق الغايات التي وجدت من أجلها ،من هنا تبرز أهمية هذا البحث كونه محاولة من الباحث لتسليط الضوء على جريمة

---

(4)عارف خليل ابو عيد ، جرائم الانترنت: دراسة مقارنه، ، مجلة جا معة الشارقة للعلوم الشرعية والقانونية المجلد٥، العدد ٣ ، صفحه ٣

(5)عرشوش سفيان جرائم المساس بأنضمة الكمبيوتر ، بحث تخرج ، المركز الجامعي خنشله –الجزائر ، معهد العلوم القانونية ، ٢٠٠٦/٢٠٠٥ ، صفحة ١٢

(6) محمود نجيب حسني، شرح قانون العقوبات ـ القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، ١٩٨٩ ، ص ٤٠

(7) محمود محمود مصطفى ، شرح قانون العقوبات القسم العام ، دار النهضة القاهره ، بدون طبعه ،١٩٧٤ ، ص٣٤

الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات لمعرفة أهم خصائصها لتطبيقها على واقع النصوص القانونية المذكور في قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠.

مشكلة الدراسة :

يهدف هذا البحث إلى دراسة الإطار العام لجريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات وفق قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ ، ومقارنتها مع التشريعات المقارنة بهدف الإجابة على التساؤلات الآتية:

أولا: ماهية جريمة الدخول غير المشروع لموقع الكتروني؟ وما هي أبرز خصائص جريمة الدخول غير المشروع لموقع الكتروني وماهي التحديات لدراسة هذه الظاهرة الإجرامية ؟.

ثانيا : ما مدى استيعاب المشرع الأردني لمخاطر الظاهرة الإجرامية للدخول غير المشروع لموقع الكتروني أو نظام معلومات الوارد نصه في المادة (٣) من قانون جرائم أنظمة المعلومات ؟

ثالثا : ماهي أركان جريمة الدخول غير المشروع؟

رابعا : ما هي أبرز الأنماط (الصور)الأكثر شيوعاً لجريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات.

أهداف الدراسة :

تهدف هذه الدراسة إلى إبراز موضوع جريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات بدراسة مستقلة عن الدراسات السابقة التي تعالج الموضوع بعمومية للوصول إلى :

أولا : مفهوم جريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات.

ثانيا : التعرف على الطبيعة الجرمية لهذه الجريمة وأركانها.

ثالثا : محل هذه الجريمة وصور النشاط الجرمي المكون لها.

رابعا : مسؤولية مرتكب هذا النوع من الجرائم المستحدثة والجزاء المقرر لها وفق نص القانون.

خامسا: معرفة حكم القوانين الجنائية المقارنة المقررة لجريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات.

سادسا: نشر الوعي لدى القانونين واطلاعهم على كل ما هو جديد في عالم الجرائم الالكترونية.

الدراسات السابقة:

قام الباحث بعملية رصد للدراسات السابقة التي تناولت موضوع الدراسة (جريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات) ، فلاحظ الباحث أن الدراسات السابقة لم تعالج موضوع الدراسة بشكل موسع ، فلم يجد الباحث في حدود اطلاعه بحثا أو دراسة أحاط بالموضوع من جميع جوانبه فقد عالجت الدراسات السابقة هذه الجريمة في إطار الجريمة المعلوماتية بشكل عام دون تحديد صورها أو تحديد ماهيتها أو أركانها ويعود السبب في ذلك إلى أن معظم الدراسات السابقة قديمة وقبل صدور قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ ولذلك تتميز دراستي عن الدراسات السابقة بمعالجة نوع محدد من أنواع الجرائم المعلوماتية بشكل تفصيلي ، تحليلي ومن كافة جوانب هذه الجريمة استنادا إلى النصوص القانونية الوارد في القانون المذكور أعلاه من خلال التطرق إلى كافة معالم هذه الجريمة وخصائصها.

منهج البحث وأدواته الرئيسية:

نظراً لطبيعة الموضوع، وغايته المتمثلة في محاولة تأصيل المفاهيم المرتبطة بالظاهرة محل البحث، فقد اعتمد الباحث على المنهج الوصفي ، المستند على البحوث المكتوبة في الموضوع كمصدر رئيس للمعلومات، ومن خلال هذه المنهجية يسعى الباحث إلى رصد، وفهم، وتحليل الظاهرة محل البحث بدقة، بهدف الوقوف على الخصائص المميزة لهذه الظاهرة.

وفي سبيل جمع المعلومات، رجعت للعديد من الدراسات السابقة في هذا المجال، كما تمت زيارة مواقع مهمة تخصصت في رصد وتتبع الظاهرة الإجرامية المتعلقة بالدخول غير المشروع لموقع الكتروني أو نظام معلومات والاستفادة من حداثة المعلومات المقدمة من خلال انتهاج المنهج المقارن بين ما توصل إليه التشريع الدولي لبعض الدول المتطورة في مكافحة الجريمة ومقارنتها مع التشريع الأردني الحديث النشأة نسبيا في مكافحة جرائم تكنولوجيا المعلومات.

خطة البحث :

نظراً لأهمية موضوع جريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات ، وارتباطه بالعديد من العناصر البشرية والمادية، ولتسارع التقنية الحديثة سواء في مجال ارتكاب الجريمة التقنية، أو في مجال قرصنة المواقع الالكترونية ، يسعى هذا البحث في جانبه الموضوعي، إلى تقديم صورة وصفية دقيقة لجريمة الدخول غير المشروع لموقع الكتروني أو نظام معلومات ، من خلال تأصيل بعض المفاهيم المرتبطة بظاهرة اختراق المواقع الالكترونية

وقرصنة البيانات بطريق غير مشروعة وفق التشريع الأردني المنصوص عليها في قانون جرائم أنظمة المعلومات لعام ٢٠١٠ ضمن أربعة فصول وخاتمه على النحو التالي:

الفصل التمهيدي فقد تناول تعريف بالمصطلحات العلمية والقانونية التي ترتبط بنظام المعلومات والمواقع الالكترونية وطرق اختراق المواقع الالكترونية ونظام المعلومات وكيفية مواجهتها وذلك في ثلاثة مباحث:

المبحث الأول : دراسة ماهية الموقع الالكتروني والبيانات والمعلومات وشبكات الحاسوب.

المبحث الثاني : تصنيفات الجرائم الالكترونية والتفريق بينهم.

المبحث الثالث: أمن الأنظمة الحاسوبية والشبكات وطرق حمايتها.

• أما الفصل الأول فيتناول جريمة الدخول غير المشروع لنظام معلومات أو موقع الكتروني بشكل مقصود وفق المادة الثالثة /الفقرة (ا) من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ ، حيث يتناول الباحث أهم خصائص هذه الجريمة و صورها ومعرفة أهم التحديات الأمنية المرتبطة بها وذلك في مبحثين:

المبحث الأول : تجريم الدخول غير المشروع إلى نظام معلومات أو موقع الكتروني.

المبحث الثاني : أركان جريمة الدخول غير المشروع لموقع الكتروني.

• أما الفصل الثاني فيتناول جريمة الدخول غير المشروع عن قصد إلى موقع الكتروني أو نظام معلومات بهدف تحقيق نتيجة جرميه حسب النصوص الواردة في قانون جرائم أنظمة المعلومات لعام ٢٠١٠وذلك في أربعة مباحث:

المبحث الأول:الركن المادي لجريمة الدخول غير المشروع بهدف تحقيق نتيجة جرمية.

المبحث الثاني : الركن المعنوي لجريمة الدخول غير المشروع بهدف تحقيق نتيجة جرمية.

المبحث الثالث:موقف التشريعات المقارنة من هذه الجريمة.

المبحث الرابع : القواعد العامة للمسؤولية عن جريمة الدخول غير المشروع لنظام معلومات والتطبيقات القضائية لها، وارتأينا أن ندرج القواعد العامة للمسؤولية عن جرائم المعلوماتية في نهاية الفصل الثاني لاعتبارات عديدة أهمها أن جرائم الدخول غير المشروع بهدف تحقيق نتيجة جرمية هي الأكثر انتشارا بين الجرائم المعلوماتية وعادة ما يقترفها أفراد الجريمة المنظمة حيث يتم توزيع الأدوار بينهم ما بين التخطيط والاشتراك الجرمي والتحريض .

• أما الفصل الثالث فيتناول الإشكالات الإجرائية لجريمة الدخول غير المشروع عن قصد لنظام المعلومات ضمن مبحثين :

المبحث الأول: الاختصاص القضائي لجريمة الدخول غير المشروع لنظام المعلومات.

المبحث الثاني: أساليب وإجراءات الضبط والإثبات والتحقيق في جريمة الدخول غير المشروع.

وفي آخر البحث خصصنا خاتمة تناولت الخلاصة العامة ونتائج هذه الدراسة، والتوصيات .

وأخيرا نرجو الله أن نكون قد وفقنا في تبيان ماهية جريمة الدخول إلى موقع الكتروني أو نظام معلومات وأركانها والإجابة على الإشكالات التي تطرحها هذه الدراسة بأسلوب علمي سهل ومميز، كما أننا نتمنى من الله سبحانه أن نكون وفقنا في وضع علامات جديدة على الطريق لبحوث لاحقة إن شاء الله.

الفصل التمهيدي

المواقع الالكترونية ونظام المعلومات وماهية الجريمة الالكترونية

الثورة المعلوماتية ترتكز على استخدام وتسخير الحواسيب الآلية والشبكات المتصلة به إما عن طريق خطوط الهواتف أو عن طريق الأقمار الصناعية بحيث تقدم خدمة الاتصال والتواصل بين الشبكات في جميع أنحاء العالم، وهذه التقنية ساهمت بشكل كبير في أن تساعد الإنسان في تقليص الوقت والمسافة وحالت دون تكبده مشقة بدنية ومادية من حيث سرعة الاتصال بالطرف الآخر دون الحاجة للتنقل أو السفر ، ولقد ساهمت شبكة الإنترنت " في تعزيز هذه الثورة وذلك بانتقال المعلومات وعدم احتكارها وانتشارها بأسرع وقت ممكن بعد القدرة الهائلة في بناء قواعد البيانات ونظم المعلومات في مواقع الكترونية مخزنة على خوادم مترابطة بشبكة عنكبوتية عالمية ، و هذه الشبكة فضاء متاح للجميع فيمكن لأي فرد أن يلج إلى هذه الشبكة في أي وقت ومن أي مكان دون حاجة لأذن مسبق من حكومة أو دولة ، بل ويستطيع أن يخاطب المجتمعات الأخرى وأن يعبر عن رأيه ويتواصل مع الآخرين دون الخوف من أن يتم مصادرة أرائه وأفكاره[٨].

المبحث الأول: ماهية الموقع الالكتروني والبيانات والمعلومات وشبكات الحاسوب

إن جريمة الدخول إلى موقع الكتروني أو نظام معلومات باعتبارها جريمة مستحدثة تستوجب توضيح المفاهيم والمصطلحات العلمية المرتبطة بها من خلال مطلبين: المطلب الأول ماهية المواقع الالكترونية وأنواعها والمطلب الثاني البيانات، المعلومات وشبكات الحاسوب.

([8]) شبكة الإنترنت يعد فضاء لا يمكن السيطرة عليه عملياً أو استحواذه واحتكاره ويمكن لكل شخص طبيعي أو معنوي من خلال هذا الفضاء أن يزاول إي نشاط يريد سواء كان هذا النشاط تجاري، فكري ، ثقافي اجتماعي ، أو سياسي أو غير ذلك من نشاطات أخرى.

المطلب الأول:ماهية المواقع الالكترونية وأنواعها

الموقع الالكتروني: هو مكان إتاحة المعلومات على شبكة الانترنت من خلال عنوان محدد[٩] ، وتعد مواقع الإنترنت أكثر أقسام الإنترنت تطورا واستخداما ، حيث تجاوز عددها في الربع الأخير من عام ٢٠٠٦ إلى ١٠٠ مليون موقع حسب ما أعلنت شركة نيتكرافت لمراقبة الانترنت مقارنة بـــ ٢٢ مليون موقع في أواخر عام ٢٠٠٠م.[١٠]

وكل موقع أو حقل يتم إنشاؤه لا بد وأن يكون له عنوان خاص به يطلق عليه اسم النطاق أو اسم الحقل أو عنوان الموقع " الدومين" ، فهو ضروري حيث يبين موقع الإنترنت لمن يسعى للوصول إليه[١١].

وعن ماهية مواقع الانترنت هناك من يري أنها عبارة عن " نظام معلومات نشط يعمل على الإنترنت له طابع اتصال عالمي متفاعل يخترق الحدود بأسلوب الربط التصويري "[١٢].

ويرتكز عمل مواقع الإنترنت على بروتوكول HTTP[١٣] الذي يسمح بربط المواقع الموصولة بشبكة الإنترنت فيما بينها. وهو لا يعمل إلا بواسطة برامج تصفح خاصةBrowsers تسمح بالاتصال بالملقمات[١٤] وبالمواقع المختلفة الموصولة بالشبكة وذلك بالاعتماد على تقنية الهيبرميديا ، وهذه الأخيرة تعد أداة مثالية للتجول في الإنترنت بفضل تقنيات الربط الفائق بين النصوص والصفحات والعناصر داخل الموقع ذاته ، وحتى بين الموقع والملقمات المختلفة الموصولة بالشبكة وذلك في إطار أو تصور يشبه بالشجرة يسمي Hypertext أوHyper link [١٥].

([9])التعريف الوارد في قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ /المادة الثانية ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

([10])عبد الرحمن بن عبدالله السند ، وسائل الإرهاب الإلكتروني " حكمها في الإسلام وطرق مكافحتها" ، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب – جدة ٢٠٠٤م ص ١٢

([11])حسين بن سعيد بن سيف الغافري ،الجرائم الواقعة على التجارة الإلكترونية ، بحث منشور على موقع منتدى المحامين العرب على الرابط http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3 ٢٠١١/١١/١٢

([12]) القرصنة الالكترونية ، مقال منشور على موقع نبض المعاني ، الرابط التالي: -http://www.nabdh alm3ani.net/nabdhat/319584-post1.html٢٠١١/١٠/١٢

([13]) بروتوكول نقل الربط الفائق Hypertext Transfer Protocol :هو بروتوكول يربط مواقع الويب الموصولة بشبكة الإنترنت فيما بينها ويسمح بالاتصال بها والتجول في عمقها باستخدام نظام الوصلات الفائقة ، أنظر الدكتور د. طوني ميشال عيسى ، التنظيم القانوني لشبكة الانترنت (دراسة مقارنة) ، دار صادر ناشرون –لبنان، الطبعة الاولى ،٢٠٠١ ، صفحه ٥١٠

([14])هو نظام حاسوبي متصل بشبكة حواسيب، أي أنه عقدة فيها، ومتخصص في أداء وظيفة معينة وتلبية الطلبات التي ترده من حواسيب أخرى على الشبكة ويسمى الخادم أو السيرفر.

([15]) طوني ميشال عيسي ، المرجع السابق ص ٦٠

وهناك من يرى في هذه الأسماء بدائل للعنوان البريدي المحدد للتعرف على شخص بعينه عبر شبكة المعلومات العالمية[١٦] ، والبعض الآخر[١٧] ينظر إليها كوسيلة تمكن مستخدمي الإنترنت من الوصول إلى المواقع عبر شبكة الإنترنت فهو عنوان للهيئات والمنظمات والمشروعات والأشخاص يمكن الوصول لها عن طريقه، وهناك من يذهب إلى أن هذه الأسماء ما هي إلا مجرد عنوان يعهد لصاحبه بحق استخدام المصطلح الذي سجله على شبكة الإنترنت[١٨] . وبهذا الاتجاه الأخير أخذت محكمة استئناف باريس في تعريفها لاسم حقل الإنترنت التجاري حينما عرفته في حكم صادر لها في عام ٢٠٠٠م بأنه" مجرد عنوان افتراضي يحدد مواقع المشروعات على شبكة الإنترنت"[١٩] . وبرأينا أن جميع هذه الآراء صحيحة لأنها ببساطه هي عنوان لشيء ما يوجد على شبكة الانترنت.

أما من الناحية القانونية فإن هذه الأسماء عبارة عن "علامة تأخذ مظهر اندماج الأرقام والحروف بحيث يتولى هذا المظهر تحديد مكان الحاسب الآلي أو موقع أو صفحة عبر شبكة الإنترنت "[٢٠]، وهو يتكون من ثلاثة مقاطع : المستوى العالي أو العام الذي يتولى تحديد طبيعة الجهة التي يتم الاتصال معها ، ومستوى ثان يتناول العلامة التجارية أو الاسم المختار أو اسم فرد ما وغيرها ، ومستوى ثالث يتناول تحديد خادم مضيف محدد يتم التعامل معه"[٢١].وموقع الإنترنت يرتبط ارتباطا وثيقا بالاسم المطلق عليه وعادة يكون بإحدى الصورتين: إما اسم عام أو دولي ، أو اسم وطني أو محلى ، وهذا معناه أن المواقع قد تكون عامة أو دولية وقد تكون وطنية أو محلية موقع الإنترنت يرتبط ارتباطا وثيقا بالاسم المطلق عليه .

([16]) محمد حسام محمود لطفي : المشكلات القانونية في مجال المعلوماتية " خواطر وتأملات" ، بحث مقدم إلى مؤتمر تحديات حماية الملكية الفكرية من منظور عربي ودولي والذي عقد في القاهرة في الفترة من ٢١-٣/٢٣/ ١٩٩٧م وذلك برعاية الجمعية المصرية لحماية الملكية الصناعية والجمعية الدولية لحماية الملكية الصناعية

([17]) حسين بن سعيد بن سيف الغافري ،الجرائم الواقعة على التجارة الإلكترونية ، بحث منشور على موقع منتدى المحامين العرب على الرابط http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3 ٢٠١١/١١/١٢

([18]) حسين بن سعيد بن سيف الغافري ،الجرائم الواقعة على التجارة الإلكترونية ، بحث منشور على موقع منتدى المحامين العرب على الرابط http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3 ٢٠١١/١١/١٢

([19]) شريف محمد غنام، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، مجلة الحقوق – جامعة الكويت، العدد الثالث ، ٢٨، سبتمبر ٢٠٠٤ - ص ١٤

([20]) عمر محمد بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، الطبعة الأولى ، دار النهضة العربية - القاهرة ، ٢٠٠٤ ،.ص ٢٢

([21]) عمر أبو بكر بن يونس ، المرجع السابق ، ص٢٢

ودراستنا لهذا المطلب سوف تكون من خلال محورين اثنين: الأول نبحث من خلاله أسماء مواقع الإنترنت العامة أو الدولية، والثاني نبحث من خلاله أسماء مواقع الإنترنت الوطنية أو المحلية، وسوف نخصص لكل محور فرع خاص به [٢٢] :

الفرع الأول: أسماء مواقع الإنترنت العامة أو الدولية

تعرف باسم نطاقات المستويات العليا ويطلق عليها اصطلاحاgeneral Top-Level Domains (gTLD) ، وهي تشير إلى أنشطة دولية عامة لا تنتمي إلى دولة بعينها وإنما توجه بالدرجة الأولى إلى المستهلكين في جميع دول العالم . وفي فترة معينة كانت هذه الأسماء تتمثل في عدد معين تغطي سبعة مجالات ثلاثة منها متاح للجميع وأربعة متاحة بشروط محددة لجهات محددة كالتالي[٢٣]:

- ثلاثة أسماء دومين متاحة للجميع للتسجيل بها وهي بلا قيد أو شرط:

.com وهو يشير إلى كل ما يتعلق بالأنشطة التجارية.

.net وهو يتعلق بالشبكات المعلوماتية.

.org ويتعلق بالمنظمات المختلفة التي لا تسعى التي تحقيق الربح.

أربعة أسماء دومين مقيد التسجيل بها وهي فئتان:

الأولى: أسماء مقصور التسجيل فيها على الهيئات الحكومية والعسكرية وهي:

.gov ويخص الهيئات المختلفة التي تتكون منها الهيئات الحكومية.

.mil وهو خاص بهيئات الدفاع العسكرية.

الثانية: أسماء مقصور التسجيل بها على من يستوفي شروط معينة وهي:

.Edu خاص بالهيئات والمعاهد التعليمية المانحة لمؤهلات دراسية.

.int وهو يتعلق بالهيئات والمنظمات الدولية المختصة بعقد الاتفاقيات الدولية.

إلى جانب هذه الأنواع السابقة تقدمت شركة(IAHC2) في فبراير١٩٩٧م بمشروع ينص على إنشاء سبعة أسماء أخرى تختلف بحسب الأنشطة وتتمثل هذه الأسماء السبعة في[٢٤]:

---

(22) القرصنة الالكترونية ، مقال منشور على موقع نبض المعاني ، الرابط التالي: -http://www.nabdh alm3ani.net/nabdhat/319584-post1.html ١٢/١٠/٢٠١١

(23) شريف محمد غنام ، المرجع السابق ، ص ٢١-٢٣.

(24) محمد حسام محمود لطفي المرجع السابق ، ص ٩٦

firm. يتعلق بالشركات التجارية ومجال الأعمال.

web. وتخص إلى الأنشطة المتعلقة بالإنترنت.

nom. تخص الأسماء والألقاب.

arts. خاص بالفن والثقافة.

info.وتشير إلى مجال بنوك المعلومات.

store. يتعلق بخدمات طلبات البضائع.

rec. خاص بأنشطة التسلية والترفيه.

وعلى الرغم من تقديم هذا المشروع إلا أنه لم يلق النور بسبب اعتراض الإدارة الأمريكية[٢٥].

وخلال عام ٢٠٠٠م وافقت مؤسسة ICANA على إضافة سبعة أسماء عامة لنطاقات عالية المستوى هي:

aero. خاصة بالنسبة للنشاط الجوي.

biz. تخص النشاط المهني.

coop. تتعلق بالنشاط التعاوني.

name. خاصة بالمواقع ذات الطابع الشخصي.

info. تتعلق بالنشاط الإعلامي وبنوك المعلومات.

museum. تخص المتاحف.

pro. تشير إلى كل ما يتعلق بالنقابات المهنية.

وفي وقت لاحق وخلال عام ٢٠٠٥م وافقت المؤسسة السالفة الذكر على استخدام اسم post. بالنسبة للنشاط البريدي. واسم travel. بالنسبة للنشاط السياحي.

الفرع الثاني: أسماء مواقع الإنترنت الوطنية أو المحلية

تعرف باسم نطاقات المستويات العليا لرموز الدول ويطلق عليها اصطلاحا country code Top-Level Domains (ccTLD) ويقصد بها تلك الأسماء التي تنتهي بحرفين يشيران إلى اسم الدولة التي تنتمي إليها هذه العناوين ، وهي لا تتقيد بحدود جغرافية فكل دولة موصولة على شبكة الإنترنت لها اسم موقع دولي فمثلا أسماء الحقول العمانية نجدها تنتهي بأول حرفين من

(25) شريف محمد غنام ، المرجع السابق ، ص ٢٩.

كلمة Oman وهو "om." ،وأسماء الحقول الأردنية تنتهي "jo" وأسماء الحقول المصرية تنتهي بـــ "eg " ، وأسماء الحقول الفرنسية تنتهي بـــ "fr " ، وأسماء الحقول الأمريكية تنتهي بـــ " us " وهكذا[٢٦] .

وغالبا ما تلجأ المشروعات إلى تسجيل عناوينها الإلكترونية أولا في مجالها الوطني فإذا ما حقق هذا التسجيل فائدة لها ، يبحث بعد ذلك عن تسجيل عنوان آخر دولي عام وغالبا ما يكون في المجالcom[٢٧].

يختلف تعريف الموقع الإلكتروني على شبكة الإنترنت باختلاف الهدف من هذا الموقع ، شركة أو مؤسسة ،فإذا كان شركة أو مؤسسة فإن تعريف الموقع الإلكتروني هو مجموعة من الصفحات الثابتة والتي تندرج تحت اسم موقع (الدومين) وهى صفحات تحتوى على معلومات عن الشركة ومقرها ونطاق نشاطها والخدمات والمنتجات التي تقدمها ومدى جودتها ووسائل الاتصال بالشركة [٢٨]، وتكون هذه الصفحات ثابتة على مدى ال٢٤ ساعة طوال أيام السنة على شبكة الإنترنت ، فهي تمثل وسيلة إعلانية عن الشركة ولكن بشكل مستمر ودون انقطاع ، وهى متاحة لجميع المتصفحين على شبكة الإنترنت من جميع دول العالم ، فبمجرد أن يقوم المتصفح بكتابة اسم الموقع على الجهاز فإنه وبنقرة واحدة يصل إلى صفحات الموقع المعني ، فلا مجال للأعطال أو التوقفات أو الأجازات مثلما يحدث مع الوسائل التقليدية للإعلان، وبذلك يكون موقع الشركة على شبكة الإنترنت هو الوسيلة الأفضل على الإطلاق لخدمة العملاء والإجابة على استفساراتهم ، بل ومن السهل بيع المنتجات والخدمات بشكل مباشر من خلال الموقع دون إضاعة للوقت أو للجهد ، هذا بالإضافة إلى العديد من الخصائص والمزايا التي يمكن إضافتها للموقع استنادًا لخدمات الشركة.[٢٩]

وهناك نوع آخر من المواقع الالكترونية يطلق عليه المواقع التفاعلية ، تكون خاصة بشخصيات عامة أو أندية رياضية أو منتديات تتوفر فيها خاصية فنية تتيح الفرصة لأعضاء الموقع للتفاعل مع الدروس والتسجيلات والتعليق عليها والتحاور مع الأعضاء بشكل مباشر ، هذان هما النوعان

---

(26) شريف محمد غنام – المرجع السابق ص ١١-١٢، الدكتور طوني ميشال عيسي – المرجع السابق ص ٦٤ ، ناتالي بورين ؛ ايمانويل جيز : اسماء مواقع الإنترنت ، مكتبة صادر ناشرون ، لبنان ، ط١ ، ٢٠٠٤م ص ٦-٩

(27) عبد الرحمن بن عبدالله السند ، المرجع السابق ، ص١٦.

(28) ما هو الموقع الإلكتروني ؟ مقال منشور على موقع داتا تكنولوجي http://kenanaonline.com/users/MST/topics/61250/posts/102134 ٢٠١١/١٠/٢٠

(29) ما هو الموقع الإلكتروني ؟ المرجع السابق: http://kenanaonline.com/users/MST/topics/61250/posts/102134 ٢٠١١/١٠/٢٠

الأكثر شيوعــــًا بين مواقع الإنترنت ، وهما الأقل من حيث التكلفة ، والأسهل في إدارتها والتعامل معها.

ويوجد العديد من أنواع المواقع الأخرى والتي تقدم خدمات مجانية أو مدفوعة ومنها موقع جوجل والذي يقدم خدمة البحث على شبكة الإنترنت أو موقع ياهو والذي يقدم خدمة البريد أو موقع الفيس بوك والذي يقدم خدمة التواصل الاجتماعي ....إلخ[٣٠].

المطلب الثاني : البيانات، المعلومات وشبكات الحاسوب

إن تحديد مفهوم البيانات والمعلومات لا يتأتى إلا من خلال التعرض لنقطتين أساسيتين: التعريف في ماهية البيانات والمعلومات والبرامج الحاسوبية كفرع أول، ونظام المعلومات والشبكات كفرع ثاني.

الفرع الأول : البيانات والمعلومات

هنالك خلط بين استعمال كلمة البيانات وكلمة المعلومات وكلمة المعرفة ، فالمعلومات تعني البيانات المجهزة ، أما البيانات فهي المادة الخام المسجلة كرموز أو أرقام ، وبمعنى آخر فالمعلومات عبارة عن بيانات تم ترتيبها بشكل أصبحت معه ذات معنى وفائدة للمستخدم ،أما المعرفة فتختلف عن المعلومات ، فالمعرفة تمثل حصيلة أو رصيد خبرة ومعلومات ودراسة طويلة يملكها شخص ما في وقت معين ، فالغرض الأساسي من المعلومات هو زيادة مستوى المعرفة وتقليل درجة عدم الثقة للمستفيد[٣١] .

تتردد كلمات البيانات (Data) والمعلومات (Information) كلما تم التطرق إلى موضوع الحاسب والجريمة الحاسوبية فما المقصود بكل منها :

---

(30) ما هو الموقع الإلكتروني ، المرجع السابق ، http://kenanaonline.com/users/MST/topics/61250/posts/102134 ٢٠١١/١٠/٢٠

(31) علم المكتبات ، مقال منشور على موقع اليسير للمكتبات وتقنية المعلومات http://alyaseer.net/vb/showthread.php?t=6687 ٢٠١١/١٠/٨

أولا: البيانات

البيانات هي مجموعة الأرقام أو الحروف أو الرموز أو الكلمات القابلة للمعالجة بواسطة الحاسب الآلي ، بعبارة أخرى البيانات هي المادة الخام التي تستقى منها المعلومات[٣٢].

وعرفها المشرع الأردني في المادة الثانية من قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ (الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها)[٣٣].

ثانيا: المعلومات

هناك عدة تعريفات لمصطلح المعلومات فيمكن تعريفها على أنها :هي المعاني التي يدركها الإنسان[٣٤] ، أو البيانات المسوغة بطريقة هادفة لتكون أساسا لاتخاذ القرار[٣٥] ، وفي تعريف آخر هي مجموعة البيانات بعد المعالجة، أي أن البيانات هي المادة الخام للمعلومات أو أن المعلومات هي مجموعة الأفكار و الحقائق التي تصف شيء أو حدث ما بعد أن تمت معالجة الأفكار والحقائق حسابياً أو منطقياً،أو غير ذلك من عمليات معالجة البيانات.[٣٦]

وعرفها المشرع الأردني في المادة الثانية من قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ (البيانات التي تمت معالجتها وأصبح لها دلالة)[٣٧]، وكذلك في المادة الثانية من قانون المعاملات الالكترونية الأردني لعام ٢٠٠١: (البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك).[٣٨]

فالمعلومات هي مجموعه من الحقائق والبيانات التي تخص أي موضوع من الموضوعات والتي تكون الغاية منها تنمية وزيادة معرفة الإنسان ، فهي أي المعلومات قد تكون عن الأماكن أو عن الأشياء أو عن الناس وبالتالي هي أية معرفة مكتسبة من خلال البحث أو القراءة أو الاتصال أو ما شابه من وسائل اكتساب المعلومات والحصول عليها[٣٩].

---

(32) أحمد فرج أحمد للدكتور أحمد فرج.، مقدمة عامة عن الحاسبات الآلية ، محاضرات منشوره على موقع بوابة الدكتور احمد فرج ٢٠١١/١١/٥
http://ahmed.farag.free.fr/documents/Cours_Informatique/Introduction_Informatique_Premier.htm

(33) http://www.lob.gov.jo/ui/laws/search_no.jsp?no=30&year=2010 20/11/2011

(34) المختصر المفيد في تعليم مباديء الحاسب الالي ، مقال منشور على http://adel900046.atspace.com/Division1.HTML ٢٠١١/١١/٥

(35) شوقى سالم . نظم المعلومات والحاسب الآلى . الإسكندرية ، مركز الاسكندرية للوثائق الثقافية والمكتبات ، ٢٠٠١ ، ص٢٩

(36) محمد نبهان سويلم، مدخل الى علم الحاسب ، المكتبة الأكاديمية -القاهره، بدون طبعه ، ٢٠٠١ ، ص٢٦

(37) المادة الثانية من قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

(38) ا لمادة الثانية من قانون المعاملات الالكترونية الاردني ،الجريدة الرسمية العدد(4524) ، بتاريخ ٢٠٠١/١٢/٣١

(39) حشمت محمد علي قاسم ، علم المعلومات بين النظرية والتطبيق ، مكتبة غريب القاهرة ، بدون رقم طبعه، ١٩٩١، ص ٧٥

ثالثا: البرامج الحاسوبية

ويمكن تعريف البرامج بأنها مجموعة من الأوامر والتعليمات الفنية المعدة لانجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات[٤٠] ، أو بعبارة أخرى تعليمات مكتوبة بلغة ما مثل لغة فيجوال سي ++ ، دلفي ، أوراكل ، جافا ...الخ ، موجه إلى جهاز تقني يسمى الحاسب الالكتروني بغرض الوصول إلى نتيجة معينة[٤١] .

وتقسم برامج الكمبيوتر من الزاوية التقنية إلى فئتين :

الفئة الأولي : برمجيات التشغيل (Operating system) ويناط بها مسؤولية عمل مكونات النظام معا وتوفير بيئة مناسبة لعمل النوع الثاني من البرمجيات وهي البرمجيات التطبيقية ، وهي تعمل كحلقة وصل بين المستخدم والأجهزة الداخلية للكمبيوتر .

الفئة الثانية: البرمجيات التطبيقية (Application Software) وهذه الأخيرة عديدة وتختلف فيما بينها باختلاف المهمة التي تقوم بها ، منها على سبيل المثال برامج معالجة النصوص و برامج الجداول أو الرسوم والبرامج التعليمية وبرامج الملتميديا وغيرها من البرامج[٤٢] .

---

(40) المادة الثانية من قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

(41)عبد الفتاح مراد شرح جرائم الكمبيوتروالانترنت ، الناشر: المؤلف ، ٢٠٠٥ ، ص ٢٢ ، انظر د. مروان مصطفى ناعسة مبادئ الحاسوب و البرمجة بلغة بيسك ، الناشر دار المسيرة عمان، ط١، ١٩٩٧ ، صفحه ١٩

(42) عبد الفتاح ، مرجع سابق ، ص ٢٣ ، انظر المحامي يونس عرب : الملكية الفكرية للمصنفات الرقمية ، دراسة منشورة على شبكة الإنترنت من خلال : www.arablaw.net

الفرع الثاني: نظام المعلومات وشبكات الحاسوب

أولا: نظام المعلومات

بشكل عام هو نظام يتكون من أشخاص وسجلات البيانات وعمليات يدوية وغير يدوية ويقوم هذا النظام بمعالجة البيانات والمعلومات في أي منظومة[٤٣]. أو هو مجموعة من العناصر المتداخلة التي تعمل مع بعضها البعض لجمع ومعالجة وتخزين وتوزيع المعلومات المتوفرة عن موضوع ما بشكل منهجي لدعم اتخاذ القرار ولدعم التنظيم والتحكم والتحليل في المنظمة وبناء تصور حالي ومستقبلي واضح عن موضوع البحث.[٤٤]

نظم المعلومات حسب ما أوردها المشرع الأردني في المادة الثانية من قانون جرائم أنظمة المعلومات لعام٢٠١٠ هي :(مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إداراتها)[٤٥].

ثانيا : تقنية المعلومات

تقنية المعلومات حسب تعريف (مجموعة تقنية المعلومات الأمريكية) ITAA، هي "دراسة، تصميم، تطوير، تفعيل، دعم أو تسيير أنظمة المعلومات التي تعتمد على الحواسيب، بشكل خاص تطبيقات وعتاد الحاسوب"، وتهتم تقنية المعلومات باستخدام الحواسيب والتطبيقات البرمجية لتحويل، تخزين، حماية، معالجة، إرسال، والاسترجاع الآمن للمعلومات.[٤٦]

أما المعلومات الإلكترونية فهي كل ما يُمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات،و بوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.[٤٧]

([43]) الموسوعة الحرة : ar.wikipedia.org/wiki/نظم_المعلومات

([44]) ماهي تقنية المعلومات ، مقال منشور ، المصدر موقع مكتوب ، http://www.mktoob.com/vb/showthread.php?p=1579 ٢٠١١-١١-٩

([45]) قانــون جرائــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

([46]) هزوان الوز، تكنولوجيا المعلومات والتجارة الإلكترونية ، مقال منشور http://www.alazmenah.com/?page=show_det&category_id=13&id=23513 ٢٠١١-١١-٩

([47]) وليد الكشباطي، جرائم اختراق الأنظمة المعلوماتيّة ، بحث منشور على http://www.chawkitabib.info/spip.php?article477٢٠١١-١١-٩

ثالثا : شبكات الحاسوب

هي سلسلة من أجهزة الكمبيوتر الموصولة معا تشارك في البيانات والبرمجيات نفسها حيث توصل إلى كمبيوتر مركزي المزوّد (server) وقد عرفها المشرع الأردني في قانون جرائم أنظمة المعلومات لعام ٢٠١٠في المادة الثانية بـــــ: (الشبكة المعلوماتية ارتباط بين أكثر من نظام معلومات للحصول على البيانات والمعلومات وتبادلها)[٤٨].

رابعا:الانترنت

الانترنت لغويا (ترابط الشبكات)، تتكون كلمة internet من كلمتين: interconnecting، network وقد أوجده الجيش الأمريكي بقصد إيجاد وسيلة اتصال موازية مستقلة وسريعة[٤٩] ، ويتكون الانترنت من عدد كبير من الشبكات الحاسب عبر routers ويحكم ترابط هذه الأجهزة وتحادثها برتوكول موحد يسمى تراسل الانترنت(Tcp)[٥٠] ، وكان الانتشار الحقيقي للانترنت عام ١٩٨٠ [٥١]تبعاً لتطوير الأجهزة الالكترونية وانتشارها في المشاريع ومنذ ذلك اليوم والانترنت ما زال ينتشر يوماً بعد يوم .

المبحث الثاني : تصنيفات الجرائم الالكترونية والتفريق بينهم

في هذا المبحث سوف نتطرق إلى تحديد ماهية جريمة الكمبيوتر ، الجريمة المعلوماتية وجرائم الانترنت بالتعريف بها ونبذة عن انتشارها والتفريق بينهما وذلك ضمن مطلبين : المطلب الأول جريمة الكمبيوتر وجريمة الانترنت ، والمطلب الثاني جرائم تقنية المعلومات.

([48]) المادة الثانية من قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦
([49]) نوال بنت علي بن محمد قيسي ، الجرائم الإلكترونية الموجهة ضد مستخدمي الإنترنت ، رسالة ماجستير، جامعة الإمام محمد بن سعود الإسلامية، العام الجامعي (١٤٣٠-١٤٣١ ه)، ص24
([50]) عبد الفتاح مراد ، مرجع سابق ، ص ٢٦
([51]). صالح أحمد البربري ، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست ٢٠٠١/١١/٢٣ صفحه١

المطلب الأول : جريمة الكمبيوتر وجريمة الانترنت

جرائم الكمبيوتر والانترنت هي جرائم تطال المعرفة ، الاستخدام ، الثقة ، الأمن ، الربح والمال ، ومع هذا كله فهي لا تطال حقيقة غير المعلومات ، لكن المعلومات – بأشكالها المتباينة في البيئة الرقمية – تصبح شيئا فشيئا المعرفة ، ووسيلة الاستخدام وهدفه ، وهي الثقة ، وهي الربح والمال ، وهي مادة الاعتبار والسمعة . إن جرائم الكمبيوتر بحق هي جرائم العصر الرقمي . تعددت التعريفات والتسميات الخاصة بالجريمة المعلوماتية مما أدى بالبعض إلى القول أن الجريمة المعلوماتية تقاوم التعريف وعليه فإن تحديد مفهوم الجريمة الالكترونية لا يتأتى إلا من خلال التعرض لنقطتين أساسيتين.

– ما هية جريمة الكمبيوتر وجريمة الانترنت.

– تصنيف الجرائم كجرائم كمبيوتر وجرائم انترنت.

الفرع الأول : ما هية جريمة الكمبيوتر وجريمة الانترنت

تعرف الجريمة عموما في نطاق قانون العقوبات – الذي يطلق عليه أيضا تسميات قانون الجزاء والقانون الجنائي [٥٢] – بأنها "فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا" [٥٣] . اخترنا هذا التعريف استنادا إلى أن التعريف الكامل –كما يرى الفقه [٥٤] – هو ما حدد عناصر الجريمة إلى جانب بيانه لأثرها. ونود ابتداء التأكيد على أهمية هذه القاعدة في تعريف الجريمة ، فبيان عناصر الجريمة (السلوك، والسلوك غير المشروع وفق القانون، الإرادة الجنائية ، وأثرها – العقوبة أو التدبير الذي يفرضه القانون) من شأنه في الحقيقة أن يعطي تعريفا دقيقا لوصف الجريمة عموما، ويمايز بينها وبين الأفعال المستهجنة في نطاق الأخلاق ، أو الجرائم المدنية أو الجرائم التأديبية.

أما جريمة الكمبيوتر ، فقد وضع لها الفقهاء والدارسون عددا ليس بالقليل من التعريفات، تتمايز وتتباين تبعا لموضع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته ، فاختلفت الباحثين في الظاهرة الإجرامية الناشئة عن استخدام الكمبيوتر من الوجهة التقنية وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية[٥٥] ، وبغض النظر عن المصطلح المستخدم للدلالة على جرائم الكمبيوتر

([52]) كامل السعيد ، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، الطبعة الثانية، دار الفكر للنشر والتوزيع ، عمان، ١٩٨٣.

([53]) محمود نجيب حسني، شرح قانون العقوبات ـ القسم العام، دار النهضة العربية، القاهرة، الطبعة السادسة، ١٩٨٩ ، ص ٤٠.

([54]) محمود حسني ، السابق ، ص ٤٠ ، و د.كامل السعيد ، السابق ، ص ٢٨.

([55]) يونس عرب ، جرائم الكمبيوتر و الأنترنيت ، المركز العربي للدراسات والبحوث الجنائية ـ ابو ظبي ١٠-١٢ /٢٠٠٢/٢ ، ص ٦

والإنترنت فإنها تندرج تحت طائفتين رئيستين : أولهما ، طائفة التعريفات على معيار قانوني ، كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة ، وتشمل أيضا تعريفات قائمة على معيار شخصي ، وتحديدا تطلب توفر المعرفة والدراية التقنية لدى شخص مرتكبها.

من التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجريم ، التعريف الذي أورده الدكتور هشام فريد رستم(٥٦): "الجريمة الإلكترونية هي كل فعل ضار يأتيه الفرد أو الجماعة عبر استعماله الأجهزة الإلكترونية، ويكون لهذا الفعل أثر ضار على غيره من الأفراد" ، وعرفها الأستاذ Rosenblatt بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه "(٥٧) وهناك من الفقهاء من عرفها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات "(٥٨) أو هي " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر "(٥٩) .

وما من شك أن معيار موضوع الجريمة كأساس للتعريف يعد من أهم المعايير وأكثرها قدرة على إيضاح طبيعة ومفهوم الجريمة.

أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة ، فان أصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة ، من هذه التعريفات ، يعرفها الأستاذ جون فورستر وكذلك الأستاذ Eslie D. Ball أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"(٦٠) وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا" (٦١)

2011-11-1http://thiqaruni.org/law/128.pdf

(56) هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، ١٩٩٢، ص ٣١
(57) هشام محمد فريد رستم ، المرجع السابق، ص ٣١
(58) هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢ ، الطبعة الأولى ص ٢٠
(59) واحد من عدة تعريفات وضعها مكتب المحاسبة العامة للولايات المتحدة الامريكية GOA انظر www.goa.gov :-
(60) Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P. 104
(61) هشام محمد فريد رستم ، المرجع السابق.، ص ٢٩ و ٣٠

وقد وجه لهذه التعريفات النقد ، من هذه الانتقادات ما يراه الأساتذة جون تابر John Taber و Michael Rostoker و Robert Rines من أن تعريف الجريمة يستدعي "الرجوع إلى العمل الأساسي المكون لها وليس فحسب إلى الوسائل المستخدمة لتحقيقه"(٦٢) ذلك أن محل الجريمة ليس المال ، وحتى بمفهوم الداعين إلى اعتبار المعلومات مالا ، فالجريمة توجه للمعلومات أساسا ، وهي قد تكون مجردة عن تجسيد أية قيمة مالية وقد تجسد في الحقيقة أموالا أو أصولا.

جانب من الفقه والمؤسسات ذات العلاقة بهذا الموضوع، وضعت عددا من التعريفات التي تقوم على أساس سمات الشخصية لدى مرتكب الفعل ، وهي تحديدا سمة الدراية والمعرفة التقنية . من هذه التعريفات ، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام ١٩٧٩ ، حيث عرفت بأنها " أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها " (٦٣) ، ومن هذه التعريفات أيضا تعريف Stein Schjqlberg بأنها " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا " (٦٤).

وفي معرض تقدير هذه التعريفات ، يمكننا القول أن شرط المعرفة التقنية ، شرط شخصي متصل بالفاعل ، وان التطور الذي شهدته وسائل التقنية نفسها اظهر الاتجاه نحو تبسيط وسائل المعالجة وتبادل المعطيات ، فلم يعد مطلوبا العلم والمعرفة العميقين ، كما انه الآن تمارس عمليات الاختراق وسرقة المعلومات باستخدام الهاتف الخلوي أنشطة أو ما يرتكب عليها من قبل أجهزة مماثلة ، كل ذلك يعكس عدم وجود ذات الأهمية للمعرفة التقنية أو الدراية بالوسائل الفنية البرمجية .

وجريمة الكمبيوتر عرّفها كذلك خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD ، بأنها " كل فعل أو امتناع من شانه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية " (٦٥) .

---

(62)هشام رستم ، المرجع السابق ، ص ٣٢.
(63) هشام رستم ، المرجع السابق ، ص ٣٢.
(64) هشام رستم ، المرجع السابق ، ص ٣٢.
(65) المصدر موقع منظمة التعاون الاقتصادي والتنمية OECD على الرابط: www.oecd.org ٢٠١١/١١/٢

والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين[٦٦] بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية ، ولأن التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح إمكانية التعامل مع التطورات المستقبلية التقنية.

وخلاصة القول أن تعريف الجريمة عموما يتأسس على بيان عناصرها المناط بالقانون تحديدها ، ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة ، بيانات ومعلومات معالجة ومخزنة ، البرامج بأنواعها ، المعلومات المستخرجة ، والمتبادلة بين النظم) وأما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزاوجة بين تقنيات الحوسبة والاتصال ، بما في ذلك شبكات المعلومات[٦٧].

الفرع الثاني: تصنيف الجرائم كجرائم كمبيوتر وجرائم انترنت

من الطبيعي في البدايات أن يكون ثمة مفهوم لجرائم ترتكب على الكمبيوتر وبواسطته قبل أن يشيع استخدام شبكات المعلومات وتحديدا الانترنت ، ومن الطبيعي أن تخلق الانترنت أنماطا جرمية مستجدة أو تؤثر بالآلية التي ترتكب فيها جرائم الكمبيوتر ذاتها بعد أن تحقق تشبيك الكمبيوترات معا في نطاق شبكات محلية وإقليمية وعالمية ، أو على الأقل تطرح أنماط فرعية من الصور القائمة تختص بالانترنت ذاتها ، ومن هنا جاء التقسيم الذي أوردناه في الفرع الأول من هذا المطلب، وان كان مبررا من حيث المنطلق فانه غير صحيح في الوقت الحاضر بسبب سيادة مفهوم نظام الكمبيوتر المتكامل الذي لا تتوفر حدود وفواصل في نطاقه بين وسائل الحوسبة (الكمبيوتر) ووسائل الاتصال (الشبكات) [٦٨].

كذلك يعتبر مخالفا للمفاهيم التقنية وللمرحلة التي وصل إليها تطور وسائل تقنية المعلومات وعمليات التكامل والدمج بين وسائل الحوسبة والاتصال ، ففي هذه المرحلة ، ثمة مفهوم عام لنظام الكمبيوتر يستوعب كافة مكوناته المادية والمعنوية المتصلة بعمليات الإدخال والمعالجة والتخزين والتبادل ، مما يجعل الشبكات وارتباط الكمبيوتر بالانترنت جزء من فكرة تكاملية النظام ، هذا من جهة ، ومن جهة أخرى تستهدف أيضا معلومات مخزنة أو معالجة ضمن أجهزة كمبيوتر أيضا هي الخوادم التي تستضيف مواقع الانترنت أو تديرها ، وإذا أردنا أن نتحكم في

---

(66) هشام رستم ، المرجع السابق ، ص ٣٥.

(67) يونس عرب ، موسوعة القانون وتقنية المعلومات ، الكتاب الاول ، قانون الكمبيوتر ، ط١ ، منشورات اتحاد المصارف العربية ، ٢٠٠١ بيروت ، ص ص ١٩٨ وما بعدها

(68) محمد سامي الشوا ، مرجع سابق ١٤٨

فصل وسائل تقنية المعلومات ، فان هذا لن يتحقق لان الشبكات ذاتها عبارة عن حلول وبرمجيات وبروتوكولات مدمجة في نظام الحوسبة ذاته ، وهذا يدخلنا في مصطلح جديد يعرف بجرائم تقنية المعلومات.

المطلب الثاني: جرائم تقنية المعلومات

في عصر المعلومات الذي نعيشه اليوم دخلت تقنية المعلومات جميع مجالات الحياة، وقد ساعد دخول شبكة الانترنت وزيادة إعداد المستخدمين لهذه التقنية على إنشاء تقنية المعلومات بشكل كبير خلال السنوات القليلة الماضية.

ولقد كان لانتشار الانترنت دور كبيرً في زيادة جرائم تقنية المعلومات لذا أصبحت الحاجة ملحة لوجود تشريع يحمى هذه القاعدة البيانية الضخمة من هذه الاعتداءات[٦٩] وهو ما أخذت به التشريعات الحديثة نسبيا ، ولمزيدا من التوضيح سوف نتناول ماهية تقنية المعلومات كفرع أول ،وخصائص جرائم تقنية المعلومات كفرع ثاني.

الفرع الأول: ماهية تقنية المعلومات

تعتبر تقنية المعلومات المعبر الحقيقي عن مضمون هذه الجريمة والسلوك الذي ظهرت على إثره لذلك كان لزاماً أن نوضح تعريف هذه التقنية التي تعني :استخدام ومعالجة البيانات آلياً باستخدام جهاز يعمل طبقاً لأوامر وتعليمات مسبقة ومحدده سلفاً يستقبل هذه المعلومات ويقوم بتخزينها، ثم معالجتها، ومن ثم استخراج ما يتطلب من نتائج مما ترتب على ذلك استخدام متزايد للآليات في العمليات الصناعية والتجارية.

كثير من الأفراد يخلطون بين هذه التقنية كجرائم وبين الحاسب الآلي وحدة كجهاز، وهذا في الحقيقة خلط غير مستساغ حيث أن الحاسب الآلي يعني ذلك الجهاز الذي يستقبل البيانات فيخزنها ثم يعالجها فيستخرج نتائجها، أما جرائم تقنية المعلومات فهي تقع بمجرد صدور أوامر إلى الحاسب الآلي فيقوم بتنفيذ هذه الأوامر وتكون نتيجة التنفيذ هي صورة الجريمة، وعليه فإن تقنية المعلومات ارتبط ظهورها، باختراع الحاسب الآلي، في حين أن البيانات التي يعالجها موجودة قبل ذلك ومع ذلك، فإنه من الخطأ من الناحية التقنية ومن الناحية القانونية، قصر نطاق النظام المعلوماتي على الحاسبات الآلية، لأنه يمكن الاستغناء عن الحاسبات الآلية والاتصال مباشرة

(69) الضرورية التشريعية تجاه جرائم المعلوماتية بحث مقدم من د. عبد الله محمد سعيد بنمة القيري في ندوة عقدت بجامعة الامارات-العين بتاريخ ٢٠١٠/١١/٢٤ تحت عنوان مكافحة جرائم تقنية المعلومات http://fl.uaeu.ac.ae 2011-11-11

بشبكة الإنترنت عن طريق الهاتف الجوال بعد تزويد الجيل الثالث من هذه الهواتف بخاصية الويب web حيث يمكن تحميل down load بعض المواقع على الهاتف الجوال[٧٠].

كذلك أيضا تشمل تقنية المعلومات النظم المطمورة embedded systems وهي عبارة عن وسيلة تستخدم في التحكم أو في مراقبة أو في مساعدة آلة أو مصنع، بحيث تصبح جزءًا لايتجزء منها، وهي تتكون من معالج دقيق أو جهاز تحكم دقيق أو دوائر متكاملة ذات تطبيق خاص، حيث تعد النظم المطمورة مبرمجة لأداء منظومة ثابتة من المهام[٧١].

أما بالنسبة لتعريف جرائم تقنية المعلومات فمن الصعوبة إيجاد تعريف لهذه الجريمة بحيث تكون محل اتفاق بين جميع من تناولها والسبب في ذلك يرجع إلى حداثة هذه الجرائم وجانبها التقني الذي لا يعلمه كثير ممن تناولوه بالدراسة، كما أن قصور بعض التشريعات في تناولها لهذه الجريمة أدى إلي عدم وضع تعريف شافي ينهي الاختلافات بين الفقهاء.

فبعض الفقهاء عرف الجريمة المعلوماتية le délit informatique :هي كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا فيه ، سواء تمثل هذا الدور في إتمام النشاط الإجرامي أو في كونه محلا له.[٧٢]

وقد عرفتها منظمة التعاون الاقتصادي والتنمية (ocde) بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، ويكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنيات المعلوماتية[٧٣] .

بعد استعراض التعريفين السابقين نلاحظ أنهما ركزتا على جانب دون آخر، ولذلك تم اللجوء إلي الرأي القائل في تعريفها ب " أنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "[٧٤].

ولم يضع المشرع الأردني في قانون جرائم أنظمة المعلومات لعام ٢٠١٠تعريفا لتقنية المعلومات بينما نجد المشرع السعودي قد أورده حسب الفقرة الثامنة من المادة الأولى من نظام مكافحة

---

[70] المواجهة الاجرائية للجرائم المعلوماتية بحث مقدم من د. أبو الوفا محمد أبو الوفا في ندوة عقدت بجامعة الامارات-العين بتاريخ ٢٠١٠/١١/٢٤ تحت عنوان مكافحة جرائم تقنية المعلومات http://fl.uaeu.ac.ae2011-11-11

[71] المواجهة الاجرائية للجرائم المعلوماتية، المرجع السابق ، http://fl.uaeu.ac.ae 2011-11-10

[72] المواجهة الاجرائية للجرائم المعلوماتية ،المرجع السابق ، http://fl.uaeu.ac.ae 2011-11-10

[73] المواجهة الاجرائية للجرائم المعلوماتية ،المرجع السابق ، http://fl.uaeu.ac.ae 2011-11-10

[74] الضرورية التشريعية تجاه جرائم المعلوماتية بحث مقدم من د. عبد الله محمد سعيد بنمة القيري في ندة عقدت بجامعة الامارات-العين بتاريخ ٢٠١٠/١١/٢٤ تحت عنوان مكافحة جرائم تقنية المعلومات http://fl.uaeu.ac.ae2011-11-11

الجرائم المعلوماتية لعام ٢٠٠٧ والتي تنص على أن المقصود بالجريمة المعلوماتية: (أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام). [٧٥]

الفرع الثاني : خصائص جرائم تقنية المعلومات

جريمة تقنية المعلومات تتميز عن غيرها بمجموعة مشتركة من الخصائص يمكن عرضها كالتالي[٧٦]:

١- صعوبة الاكتشاف والإثبات:

جرائم تقنية المعلومات جرائم لا عنف بها ولا توجد آثار لاقتحام، وإنما هي عبارة عن جملة من الأرقام والبيانات التي تتعرض لاعتداء أيا كانت صورته هدفه تغيير أو محو من السجلات المخزنة دون ترك أي أثر خارجي [٧٧].

٢- هذه الجرائم لا تترك أثراً مادياً في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن بعض مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة[٧٨].

٣- يختلف موضوعها باختلاف مراحل تشغيل نظام المعالجة الآلية للبيانات.

تمر عملية تشغيل نظام المعالجة الآلية للبيانات بمراحل ثلاث، ولكل مرحلة من هذه المراحل نوعيه خاصة من الجرائم لا يمكن وفقاً لطبيعتها ارتكابها إلا من خلال هذه المرحلة، فمثلاً خلال مرحلة الإدخال يمكن إدخال بيانات غير صحيحة، وعدم إدخال وثائق أساسية، وهذه المرحلة تعتبر من أعظم المراحل التي ترتكب فيها جرائم تقنية المعلومات، وكذلك في مرحلة المعالجة يمكن إحداث خلل أو إلغاء جزئي أو كلي لعمل البرامج الأصلية وجرائم هذه المرحلة تتصف بصعوبة الاكتشاف، أما في مرحلة الإخراج فيتم التلاعب في النتائج التي تم التوصل إليها عن طريق معالجة بيانات صحيحة بطريقة غير صحيحة.

٤- التفتيش في هذا النمط من الجرائم التي يتم عادة على نظام الحاسوب وقواعد البيانات وشبكات المعلومات، وقد يتجاوز النظام المشتبه به إلي أنظمة أخري مرتبطة، وهذا هو الوضع الغالب من خلال التشبيك بين الجوانب وانتشار الشبكات الداخلية على مستوى الدول. وامتداد التفتيش إلي

---

[75] وزارة الإتصالات و تقنية المعلومات. "نظام مكافحة جرائم المعلوماتية ."
http://www.mcit.gov.sa/arabic/Regulations/CriminalLaws ٢٠١١/١٠/٢٠

[76] الضرورية التشريعية تجاه جرائم المعلوماتية بحث مقدم من د. عبد الله محمد سعيد بنمة القيري في ندة عقدت بجامعة الامارات-العين بتاريخ ٢٠١٠/١١/٢٤ تحت عنوان مكافحة جرائم تقنية المعلومات http://fl.uaeu.ac.ae

[77] محمد حمّاد الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، دار الثقافة عمان ٢٠٠٤، ط ١ ، ص ١٦٦

[78] محمد خليفه ،الحماية الجنائية لمعطيات الحاسوب الالي ، دار الجامعة الجديدة ، الطبعة الاولى ، ٢٠٠٧ ، ص٣٤

نظم غير النظام محل الاشتباه يخلق تحديات كبيرة من حيث مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

٥- أدلة الإدانة في جرائم تقنية المعلومات ذات نوعية مختلفة فهي مضوية الطبيعة مثل سجلات الحاسوب، معلومات الدخول، وهذه الأدانه قد تثير مشاكل أمام القضاء من حيث مدى قبولها، وحجتها والمعايير المتطلبة لذلك(٧٩)، لذلك فالبعد الإجرائي لجرائم الحاسوب والانترنت ينطوي على تحديات ومشكلات جمة يتطلب الأمر فيها الإسراع إلي الكشف خشية ضياع الدليل، وخصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم.

المبحث الثالث : أمن الأنظمة الحاسوبية والمواقع الالكترونية وطرق حمايتها

لقد نمت الإنترنت بشكل مذهل خلال السنوات العشر الأخيرة ، فبعد أن كانت مجرد شبكة أكاديمية صغيرة أصبحت تضم الآن ملايين المستخدمين في كافة المدن حول العالم وتحولت من مجرد شبكة بحث أكاديمي إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات ، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها ، ولهذا لم يتم بناء الشبكة في المراحل الأولى على نحو يراعي تحديات أمن المعلومات ، فالاهتمام الأساسي كان يركّز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة . وسوف نتناول هذا المبحث في مطلبين أمن المعلومات والمشاكل الأمنية لشبكات الحاسوب كمطلب أول و اختراق المواقع الالكترونية وأنظمة المعلومات والحماية لها كمطلب ثاني.

المطلب الأول : أمن المعلومات والمشاكل الأمنية لشبكات الحاسوب

الإنترنت سلاح ذو حدين، فهو مدخل للكثير من الأشياء النافعة، ولكن مع الأسف، فهو يفتح المجال أمام الكثير من الأشياء المؤذية للدخول إلى النظام المعلوماتي. وثمة العديد من المسائل الأمنية الواجب الاعتناء بها للإبقاء على سلاسة تشغيل أجهزة الكمبيوتر والشبكات(٨٠).

---

(79) الضرورية التشريعية تجاه جرائم المعلوماتية ، المرجع السابق ، http://fl.uaeu.ac.ae

(80)امن المعلومات ، مقال منشور ، تاريخ الزياره ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

في البداية لا بد من الإشارة إلى إن شركة مايكروسوفت اتبعت خطوات رائدة لتحقيق الحماية لبرامجها ومن أهم التقنيات التي تستخدمها لحماية برامجها product actuation بهدف تقليل قرصنة البرامج خاصة ما يعرف بsoft lifting or casual copying وهذه التقنية لا تحتاج أي بيانات شخصية إضافية من المستخدم فهي فقط تحتاج إلى بيانات معينة مثل رقم هوية التحميل ورقم هوية المنتج (٨١).

لذلك يجب اخذ الحيطة والحذر الدائمين لحماية النظام الحاسوبي حتى لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكن تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً وسنأتي عليها بالتفصيل لاحقا..

واستنادا إلى ما سبق سوف نتعرف على ماهية أمن المعلومات " فرع أول" وأهم المشاكل الأمنية لشبكة المعلومات" فرع ثاني".

الفرع الأول : أمن المعلومات

إن مصطلح امن المعلومات سابق على وجود التقنيات المعلوماتية المرتبطة بالكمبيوتر،إلا أن الصدارة التي احتلتها التقنيات الحديثة في سرعة النقل والاتصال والتخزين هي التي جعلت هذا المصطلح أكثر ارتباطا بالمعلومات حيث يتم تعريفها : بأنها الأساليب والوسائل المعتمدة للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من السرقة والنسخ والتشويه والابتزاز والتلف والضياع والتزوير والاستخدام غير المرخص وغير القانوني، وتجهيز البدائل لمجابهة أي تهديد حقيقي(٨٢).

وتعني أمن المعلومات إبقاء المعلومات تحت السيطرة المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن من صاحبها، وان يكون لدى صاحب الموقع علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى المعلومات الخاصة.

من الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من

---

(81) عبد الصبور عبد القوي ، الجريمة الالكترونية ، دار العلوم للنشر والتوزيع ، الطبعة الاولى ، ٢٠١٠، ص١١٩

(82) " تحديات السلامة المعلوماتية وحما ية الفضاء المعلوماتي والامكانات التي يتيحها الفضاء المعلوماتي الآمن"، ورقة مقدمة من قبل الدكتور عاصم علي الجدوع الى مؤتمر الامن والسلامة المعلوماتية الذي عقد في الجامعه الاردنية في الفترة من ٢١-٢٣/١١/٢٠١١

الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات[٨٣].

وغالبا ما تتيح مواطن الضعف في شبكة الانترنت للمهاجم إمكانية التحايل على البرنامج بتجاوز فحص إمكانية الوصول أو تنفيذ الأوامر على النظام المضيف لهذا البرنامج، ويمكن إجمالها كالتالي:

أولا : مواطن الضعف في شبكة الإنترنت

تعتبر شبكة الإنترنت عرضة للعيوب والضعف في دفاعاتها ،وهناك عدد من نقاط الضعف والتي يكون جهازا لحاسوب أو الشبكة عرضة لها. ومن أكثرها شيوعا هي أخطاء تدقيق صحة إدخال البيانات مثل الأخطاء البرمجية الناجمة عن تنسيق الرموز النصية، والتعامل الخاطئ مع الرموز المتغيرة لغلاف البرنامج ولذلك يتم تفسير هذه الرموز، وإدخال عبارات SQL وتضمين النصوص برمجية متعارضة،ومن نقاط الضعف الشائعة أيضا تحطم المكدس وفيض البيانات في ذاكرة التخزين المؤقت بالإضافة إلى ملفات الروابط الرمزية (Symlinks).

ثانيا : فحص مواطن الضعف

يمكن أن تكون هناك نقاط ضعف في جميع أنظمة التشغيل مثل الويندوز، ماكنتوش، لينوكس، OpenVMS، وغيرها. ويمكن فحص نقاط الضعف في الشبكة والخوادم من خلال إجراء اختبار خاص عليها يتم من خلاله فحص الخوادم والصفحات الإلكترونية وجدران النار وغير ذلك لمعرفة مدى تعرضها لنقاط الضعف. ويمكن تنزيل برامج فحص نقاط الضعف من الإنترنت[٨٤].

الفرع الثاني: المشاكل الأمنية

تحدث المشكلة الأمنية عندما يتم اختراق النظام الحاسوبي من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة.

وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة. ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.

([83]) امن المعلومات ، مقال منشور ، تاريخ الزياره ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

([84])امن المعلومات ، مقال منشور ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد (غير المصرح لهم) إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام. كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطل الجهاز مؤقتاً، إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة[٨٥]. وتاليا أهم الأشياء التي تسبب مشاكل أمنية على شبكة المعلومات:

أولا : الهاكرز

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي. وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة ومعظمهم محترفون[86].

ثانيا: الكراكرز

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية ، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها ، ولذلك فان هذه الطائفة تعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الكمبيوتر كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي .

والفرق بين الهاكر والكراكرز يكمن في أن الكراكرز يسعون لسرقة معلومات حساسة من جهات تجارية أو حكومية وذلك بغرض بيعها على جهات أخرى تهمها تلك المعلومات ومنهم العاملون في الجريمة المنظمة وبالتالي هؤلاء يختلفون عن الهاكر بأنهم يخترقون من اجل التربح المالي بعكس الطائفة السابقة فهدفهم التطفل والفضول واثبات القدرات[٨٧].

---

[85] امن المعلومات ، مقال منشور ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar
[86]امن المعلومات ، مقال منشور ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar
[87] الدكتور عبد الفتاح مراد ، المرجع السابق ،صفحه ٤٧

وهناك من يرى أن الفرق بين الهاكر والكراكرز على أساس أن الأول له القدرة على اختراق الأجهزة الحاسبات فيسمى مخترق وإما الثاني فهو له القدرة على اختراق الحاسب المحمي ولكنه يقوم بحذف ملفات أو تشغيل آخر فهو مخرب [٨٨].

ولكنني شخصيا أؤيد الاتجاه الأول خصوصا إن بعض الدراسات والمعالجات في حقل جرائم الكمبيوتر والانترنت،بل بعض التشريعات المحلية في الولايات المتحدة الأمريكية – تعتمد هذا التمييز ، فاصطلاح الكريكرز مرادف للهجمات الحاقدة والمؤذية في حين إن اصطلاح الهاكر مرادف في الغالب لهجمات التحدي طبعا دون أن يؤثر هذا التمييز على مسؤولية مرتكبي الأنشطة من كلا الطائفتين ومساءلتهم عما يلحقونه من أضرار بالمواقع المستهدفة باعتداءاتهم[٨٩].

ثالثا: فيروسات الكمبيوتر

فيروسات الكمبيوتر هي برامج كمبيوتر مصممة للعمل على جهاز الكمبيوتر دون إذن من مالكها والتداخل مع عمليات وسجلات الكمبيوتر وتخريب أو حذف المعلومات أو حتى استغلال موارد النظام لأغراض تخريبية أخرى[٩٠].

أما برامج الإعلانات (adware) فهي مصممة للدعاية والإعلان وتغيير الإعدادات العامة في أجهزة الكمبيوتر التي تتغلغل فيها. أما برامج التجسس (spyware) فهي برامج تقوم بتجميع الأنشطة المختلفة التى تمارس على شبكة الانترنت وعلى المواقع الإلكترونية التي يتم زيارتها ، حيث يقوم البرنامج بإرسال المعلومات التى تم تجميعها إلى جهاز خادم أو server محدد[٩١].

رابعا : اللصوصية (Phishing)

أخذت هذه التسمية من كلمة Fishing والتي تعني صيد السمك [٩٢]، ويمكن تعريفها على أنها سرقة البيانات الشخصية السرية والحساسة عن طريق رسائل البريد الالكتروني لغرض انتحال الشخصية[٩٣].

---

[88] عبد الصبور عبد القوي ، المرجع السابق ، ص٦١

[89] يونس عرب ، المرجع السابق ، ص٨٣

[90] امن المعلومات ، مقال منشور ، 15/11/2011 http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

[91] امن المعلومات ، المرجع السابق ، ٢٠١١/١١/١٥ http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

[92] محمد عبد الله المنشاوي ، جرائم الانترنت في المجتمع السعودي ، رسالة ماجستير ، جامعة الملك سعود، الرياض ٢٠٠٣/٤/٢٩ ، ص٦٧

[93] الاصطياد الالكتروني : الاساليب والاجراءات المضادة ، خالدبن سليمان الغثبر، سليمان عبد العزيز الهيشه ، مركز التميز لامن المعلومات ، نسخة الكترونية ،ص٣٩ على http://coeia.edu.sa/index.php/ar/asuurance-awarness/books-in-information-security/786-phishing-book.html ٢٠١١/١١/٢٠

يستخدم مصطلح (Phishing) للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول إلى الموقع[٩٤].

تعتبر رسائل البريد الالكتروني الأكثر شيوعا في تنفيذ هجمات الاصطياد الالكتروني (Phishing)[٩٥] ،وهناك برامج لمكافحة الاصطياد الالكتروني مثل (security software) ،وتستخدم ضد هجمات التصيد الالكتروني بنوعيها المعتمد على الرسائل الالكترونية ، أو المعتمد على استغلال الثغرات الأمنية[٩٦] .

وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي.

وللاستدلال على حجم الخسائر التي يمكن أن تسببها هجمات الاصطياد الالكتروني عن طريق البريد الالكتروني ، نشرت (Gartner) أن الخسائر في الولايات المتحدة الأمريكية الناتجة عن هجمات الاصطياد الالكتروني قد ارتفعت لتصل في عام ٢٠٠٧ إلى ٣,٢ بليون دولارامريكي[٩٧].

خامسا: البريد الإلكتروني

يجدر بنا أن نتذكر دائماً إلى أن البريد الإلكتروني لا يضمن الخصوصية، فخصوصيته تشابه خصوصية البطاقة البريدية. ويتنقل البريد الإلكتروني في طريقه إلى المستلم عبر العديد من الخوادم حيث يمكن الوصول إليه من قبل الأشخاص الذين يديرون النظام ومن الأشخاص الذين يتسللون إليه بشكل غير نظامي. والطريقة الوحيدة للتأكد إلى حد ما من خصوصية البريد الإلكتروني هو تشفيره.

---

[94] امن المعلومات في الاجهزة المحمولة -http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/51-forensic-and-computer-crimes/1324-information-security-in-mobile-devices11.html 2011-11-10

[95] A. Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", Radix Labs, October 3, 2005.

[96] الاصطياد الالكتروني،المرجع السابق ، صفحه ٥٥

[97] الاصطياد الالكتروني،المرجع السابق ، صفحه ٥٥

المطلب الثاني :اختراق المواقع الالكترونية وأنظمة المعلومات والحماية لها

ودراستنا لهذه الظاهرة سوف تكون من خلال محورين اثنين: الأول نبحث من خلاله ماهية الاختراق الالكتروني للمواقع الالكترونية، والثاني نبحث من خلاله وسائل حماية أنظمة المعلومات والمواقع الالكترونية، وسوف نخصص لكل محور فرع خاص به.

الفرع الأول : اختراق المواقع الالكترونية

قضية اختراق المواقع الالكترونية هي واحدة من القضايا التي تقع تحت طائلة القانون ، والتي تندرج تحت قائمة الجرائم المعلوماتية ، والاختراق بشكل عام هو: القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف[٩٨] وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين عنوه ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو بنفسياتهم عند سحبه ملفات وصور تخصهم وحدهم.

تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الإختراق ، ولكنها جميعا تعتمد على فكرة توفر اتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم (server) الخاص بالمخترق ، وجهاز المخترق على الطرف الأخر حيث يوجد برنامج المستفيد أو العميل Client.

ويشمل الاختراق أجهزة الحاسوب وشبكاتها والمواقع الالكترونية على اختلافها والأجهزة الخلوية . وللأسف الشديد بدأت جريمة اختراق المواقع الالكترونية تأخذ إشكالا كثيرة لأهداف عديدة لها بواعثها الخاصة ، الأمر الذي يزداد سوءا عندما تنتشر بين الشباب بهدف قياس درجة احترافه وقدرته على اختراق الشبكة العنكبوتية دون الوعي بعقوبتها القانونية .

وفيما يتعلق باختراق المواقع الالكترونية فقد تتعددت وسائل وأساليب اختراق المواقع الإلكترونية ، إلا أنها في مجملها تهدف إلى مهاجمة هذه المواقع وتحقيق نفع معين للمهاجم من وراء ذلك ، وفي بعض الأحيان لا يكون هناك نفع للمهاجم سوى تعريض الموقع الضحية للخطر والضرر . واختراق المواقع الالكترونية يكون بعدة أساليب وطرق منها :

([98]) جرائم الحاسوب"، ورقة مقدمة من قبل النقيب المهندس رائد بلاسمه الى مؤتمر الامن والسلامة المعلوماتية الذي عقد في الجامعه الاردنية في الفترة من ٢١-٢٣/١١/٢٠١١

أولا: تدمير المواقع

تدمير الموقع الالكتروني يقصد به الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي (server-pc) أو مجموعة نظم مترابطة شبكيا بهدف تخريب نقطة الاتصال أو النظام(٩٩).

ومن الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمعتدي إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع ، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي(١٠٠).

والجدير بالذكر أن هجومين من هذا النوع تعرض لها موقع Hotmail وذلك في أواخر عام ٢٠٠٠م ، وتسبب في خسائر مالية تجاوزت ملايين الدولارات(١٠١) .

ثانيا : تشويه المواقع Defacement

يوجد تشابه كبير، بين ما يحصل في العالم الافتراضي من عمليات تشويه مواقع الويب (Defacement)، وبين ما يحدث على أرض الواقع عندما يتم إنزال علم دولة معينة، من السفينة، ورفع علم القراصنة مكانه، حيث أن عملية التشويه، في أغلب الأحيان، ليست سوى تغيير الصفحة الرئيسية للموقع، بصفحة أخرى، يعلن المخترق فيها انتصاره على نظام مزود ويب والإجراءات الأمنية للشبكة، ويقصد من ورائها إبراز قدراته التقنية، وإعلان تحدّيه للمشرفين على نظم مزودات ويب، ليثبت لنفسه، أو لغيره، امتلاكه المقدرة التقنية على كسر نظام الحماية في هذه المزودات، الأمر الذي يتطلب معرفة معمقة لطريقة عمل الانترنت، وبروتوكولات التشبيك، وأنظمة التشغيل المختلفة التي تعمل عليها مزودات ويب، وتتضمن الصفحة الجديدة أحياناً رسالة يرغب الشخص الذي قام بعملية التشويه إيصالها للعالم. وقد تتضمن هذه الرسالة

---

(99) حسين بن سعيد بن سيف الغافري الجرائم الواقعة على التجارة الإلكترونية ، سلطنة عمان مسقط ٢٠٠٦
2011-11-12http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3

(100) عبد الرحمن بن عبدالله السند : وسائل الإرهاب الإلكتروني " حكمها في الإسلام وطرق مكافحتها" ، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب ، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية ٢٠٠٤م ص١٦-١٧

(101) حسين بن سعيد، الجرائم الواقعة على التجارة الالكترونيه ،سلطنة عمان مسقط ٢٠٠٦
2011-11-12http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3

اعتراضاً منه على حالة سياسية أو اجتماعية، أو صرخة يريد إيصالها، إلى كل من يزور هذا الموقع[١٠٢]!

وتقتصر الأضرار التي تتسبب بها عمليات تشويه مواقع ويب، على الإضرار بسمعة الجهة المالكة للموقع،حيث يتم تغيير الصفحة الرئيسية فقط من الموقع بصفحة HTML من تصميم المخترق، ولا يلجأ المخترقون عادةً في عمليات التشويه إلى تدمير محتويات الموقع، حيث يستطيع الآخرون زيارة المواقع التي تتعرض لعمليات التشويه والوصول إلى جميع صفحاته المكونة للموقع.

يتّبع المخترقون عادة أساليب عدة في عمليات تشويه صفحات ويب، وتختلف هذه الأساليب من موقع إلى آخر، بناءً على نوع نظام التشغيل، ومزود ويب الذي يعتمد عليه الموقع، وهنا نذكر أكثر هذه الأساليب انتشاراً وهي :

أ. الدخول بهوية مخفية (anonymous) عبر منفذ بروتوكول FTP

هذه الطريقة تمكّن المخترق في بعض الحالات من الحصول على ملف كلمة الدخول المشفرة الخاصة بأحد المشرفين على الشبكة، أومن يملكون حق تعديل محتويات الموقع، والعمل على فك تشفيرها، فمن شأن حصول المخترق على كلمة السر الخاصة لأحد المشرفين، السماح له بالدخول إلى مزود ويب، وتغيير الصفحة الرئيسية[١٠٣].

ويلجأ المخترقون، بعد الحصول على ملف كلمة السر، إلى استخدام برامج خاصة لتخمين كلمات السر[١٠٤].

ب. استغلال الثغرات الأمنية في مزودات ويب، وأنظمة التشغيل

لا يخلو أي نظام تشغيل، أو مزود ويب من ثغرات أمنية تعرض مستخدميه لخطر الاختراق، ويعمل المطورون بشكل مستمر على سد هذه الثغرات كلما اكتشفت، ويستغل الهكرة هذه الثغرات الأمنية في عمليات الاختراق، إلى أن تجد الشركة المصممة للنظام الحل المناسب لها، وتبقى بعض الثغرات متاحة لفترة طويلة حتى يتم اكتشافها، وذلك لأن أغلب الثغرات التي يكتشفها الهكر، لا يعلنون عنها بسرعة، ليتمكنوا من استغلالها فترة أطول،لأجل ذلك ينبغي على جميع

---

(102) حسين بن سعيد، الجرائم الواقعة على التجارة الالكترونيه ،سلطنة عمان مسقط ٢٠٠٦
2011-11-12http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3

(103) إختراق المواقع وطرق الوقاية – دراسة منشورة على شبكة الإنترنت بتاريخ ٢٠٠٥/٩/٦ من خلال موقع
:www.websy.net/learn/hackers/course44.htm 2011-11-12

(104) من أكثر هذه البرامج انتشاراًCracker Jack :، وJohn The Ripper، وJack The Ripper، وBrute ForceCracker

مدراء ومشرفي الشبكات، متابعة مواقع الشركات المصممة لنظم التشغيل، ومزودات ويب، ليتسنى لهم الإطلاع على آخر ما تم التوصل إليه من ثغرات أمنية، وجلب برامج الترقيع (patches) لها ، حيث تحرص هذه الشركات على تقديم مثل هذه البرامج بأسرع وقت ممكن(١٠٥).

ثالثا: حجب الخدمة (Denial of serviceDoS)

" الوصول إلى هذا الموقع، غير ممكن! " قد تعني الرسالة السابقة أن الموقع الذي تحاول أن تزوره، تعرض لهجمات حجب الخدمة، خاصة إذا كان واحداً من المواقع الكبرى، التي يعني ظهور مثل هذه الرسالة في موقعها، خسارة عشرات الآلاف من الدولارات في كل ساعة ويتم ذلك عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن طريق أجهزة مصابة ببرامج(في هذه الحالة تسمى DDOS Attacks) ، بحيث يتحكم فيها القراصنة والعابثين الإلكترونيين لمهاجمة المواقع الإنترنت عن بعد لإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحامًا مروريًا بهذه المواقع ويسبب صعوبة وصول المستخدمين لها نظرًا لهذا الزحام(١٠٦).

رابعا: محاكاة المواقع

غالبا ما يستخدم هذا الأسلوب في السطو على أرقام البطاقات الائتمانية وأرقام الحسابات والأعمال التجارية، وفكرته تقوم على تقليد أحد المواقع الحقيقية التي غالبا ما تكون مواقع تجارية بكافة تفاصيلها من تخطيط وألوان وتصميم. وعادة ما يتم عن طريق تسجيل اسم نطاق يكون وثيق الصلة بمواقع سليمة قانونا وربما يختلف في حرف واحد ، بعدها يقوم موقع الويب غير القانوني بنسخ بعض محتويات الموقع القانوني وينشئ بعض الوظائف بغرض تقليد الإحساس بالروابط المحتواة في الموقع ، والخطوة الثالثة تكمن في تقديم منتج عام بسعر مدهش لحث الناس على إرسال معلوماتهم الائتمانية(١٠٧).

---

(105) حسين بن سعيد، الجرائم الواقعة على التجارة الالكترونيه ،سلطنة عمان مسقط ٢٠٠٦
2011-11-12http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3

(106) حسين بن سعيد، الجرائم الواقعة على التجارة الالكترونيه ،سلطنة عمان مسقط ٢٠٠٦
2011-11-12http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3

(107) الدكتور:محمد نور شحاته:التجارة الإلكترونية،بحث منشور بتاريخ ٢٠٠٥/٥/١٥م على شبكة الإنترنت:
2011-11-12www.eastlaws.com

خامسا: انتحال شخصية الموقع

يتم بهجوم يشنه الهاكرز على الموقع والسيطرة عليه ومن ثم يقوم بتحويله لموقع آخر . أو يحاول الهاكرز اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرامج الخاصة به هناك . مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور[١٠٨].

سادسا : الاعتداء على أسماء حقول الإنترنت " الدومين" Domain Name

اسم النطاق أو الميدان أو الموقع (دومين نيم – Domain name) هو في الحقيقة عنوان إنترنت ، فالعنوان البريدي له رقم صندوق مميز ورمز منطقة مميز مثلا(وسط البلد ص.ب ٢٣٢٥ رمز ١١١١٨) وللإنترنت أيضا عنوان مميز (www.ju.edu.jo/arabichome.aspx) بعض الاختراقات يقوم فيها المخترق دون المساس بالموقع ظاهرا وهناك نوع آخر من الاختراقات وفيه يقوم المخترق بسرقة (الدومين) أي عنوان الموقع والسيطرة عليه ولا يستطيع صاحب الموقع الدخول إلى ملفات موقعه ويصبح في سيطرة المخترق.

وقد احتدم النزاع حول أسماء نطاقات الانترنت ، ومعمارية شبكة الانترنت والجهات التي تسيطر عليها ، وقد حسم جانب من الجدل مؤخرا حول إضافة مميزات جديدة للميزات المشهورة (com,net,org,gov,edu) وذلك بإقرار إضافة سبعة مميزات أخرى ، ويرجع الخبراء مشكلات أسماء النطاقات في بيئة الانترنت إلى استراتيجيات الشركات الكبرى في هذا الشأن ، فهي التي قادت لواء معارضة توسيع أسماء النطاقات ، حماية لأسمائها التجارية[١٠٩].

إن أسماء الحقول – الدومين– بوصفها علامة لتميز السلع والخدمات عبر شبكة الإنترنت ، تتمتع بالحماية القانونية المقررة طبقا لمبدأ أسبقية التسجيل، بمعنى أنه في حالة التزاحم بين عدة شركات أو أشخاص لهم ذات الاسم بالنسبة لأحد السلع والخدمات ، فإن الحماية القانونية المقررة تكون لمن بادر وسبق غيره في التسجيل[١١٠].

---

[108] المستشار . محمد محمد الألفي : أنماط جرائم الإنترنت ، بحث منشور على شبكة الإنترنت بتاريخ ٢٠٠٥/٩/٢٤م من خلال موقع www.eastlaws.com 2011-11-12

[109] يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية ،ورقة عمل مقدمة امام الندورة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي – دمشق
www.lawjo.net/vb/attachment.php 2011-11-12

[110] حسين بن سعيد، الجرائم الواقعة على التجارة الالكترونيه ،سلطنة عمان مسقط ٢٠٠٦
http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3 2011-11-12

الفرع الثاني : وسائل حماية أنظمة التشغيل والمواقع الالكترونية

سنستعرض في الفقرات التالية لمزيد من المعلومات حول البرمجيات المختلفة والوسائل المتعلقة بالأنظمة الأخرى للإبقاء على المعلومات آمنة، لكن علينا أن نتذكر أن ثمة العديد من الطرق الأخرى التي يسلكها المتسللون للوصول إلى المعلومات، لذلك يجب وضع الكمبيوتر الخاص بنا وخصوصاً الكمبيوتر المحمول في مكان آمن، وحمايته بكلمة مرور ويستحسن إغلاقه خصوصا عندما نكون بعيدين عنه. ويجب عدم إعطاء أي شخص يرغب في الحصول على أي من كلمات المرور الخاصة ، حتى لأولئك الأشخاص الذي يعملون (أو يدعون بأنهم يعملون) في الدعم الفني في الموقع.

وهناك عدة وسائل تتخذ لحماية المواقع وأنظمة التشغيل منها:

أولا: التحديثات

يجب تحديث جميع برامج تشغيل النظام بأحدث نسخة من برنامج التشغيل الذي تستخدمه. وعادة ما يستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، ويعد تركيب آخر التحديثات الأمنية لأنظمة التشغيل (operating systems) ، ومتصفحات الشبكة العالمية (Internet Browsers) ، إجراء مضادا فعالا ضد هجمات التصيد الالكتروني المعتمدة على استغلال الثغرات الأمنية(١١١) .

ثانيا: جدار النار (Firewall)

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين، وتختلف جدران النار حسب احتياجات المستخدم. علماً بأن الكثير من الشبكات والخوادم تأتي معها نظام جدار حماية ناري افتراضي، ولكن ينبغي التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي يحتاج إليها النظام المعلوماتي، فإن لم يكن قادراً على ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

ثالثا: التشفير

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس، بمعنى أن تشفير المعلومات في الجهاز يجعلها غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة

---

(111) خالدبن سليمان الغثبر، سليمان عبد العزيز الهيشه ، المرجع السابق ، صفحه ٩٢

إلى النظام دون إذن، ويتم حماية الشبكة اللاسلكية باستخدام بروتوكول تشفير الشبكات اللاسلكية (WEP). ويعمل هذا البروتوكول بتضمين مفتاح مشترك ٦٤ أو ١٢٨ بت بين العملاء ونقطة الدخول، ومن ثم يتم استخدام هذا المفتاح لتشفير وفك تشفير البيانات بينهم، وهذا يوفر قدر كاف من الأمن للشبكات المنزلية ،أما بالنسبة لبيئات الشركات، فيجب اعتبار هذا البروتوكول (WEP) فقط كنقطة بداية للترتيبات الأمنية، وعلى الشركات البحث جدياً في ترقية شبكاتهم اللاسلكية إلى مستوى (WPA) أكثر أماناً، ومن أشهر برامج التشفير (PGP)[١١٢] .

رابعا : التعريف

يكون للأجهزة ومديرو الشبكات أسماء تعريف افتراضية في النظام، ومن السهل كثيراً على الهاكر إيجاد هذه الأسماء، ومن ثم عمل كلمات مرور واسم مستخدم شخصي لمديري الشبكات من خلال تعديل أسماء التعريف الافتراضية في النظام. لذا ننصح بإعطاء الأجهزة أسماء لا تكشف عن هوية صاحبها أو أماكنها، ومثال ذلك بدلاً من استخدام العنوان الفعلي مثل اسم المبنى أو اسم الشركة كأسماء للاجهزه، يمكنك استخدام أسماء مختلفة مثل "الجبل Mountain" أو "جهازي My Device".

خامسا: برامج مراقبة بيانات الشبكة Packet Sniffers

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة[١١٣].

سادسا : .ترشيح العناوين MAC filtering

يعرف عنوان (MAC) كذلك بأنه العنوان المادي، وهو معرّف فريد لكل جهاز في الشبكة. ويعني مصطلح ترشيح العناوين أن يقوم مدير الشبكة يدوياً بإدخال قائمة بالعناوين الموجودة في الشبكة المحلية ومن ثم يقوم بإعداد الموجه (router) ليسمح فقط بتوصيل هذه العنوانين المحددة عبر الشبكة اللاسلكية، ويمكن بسهولة العثور على العناوين (MAC Addresses) من خلال

---

(112) انظر موقع symantec http://www.pgp.com 9/11/2011

(113) امن المعلومات ، مقال منشور ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

الذهاب إلى مؤشر الأوامر (Command Prompt) في كل نظام وكتابة هذه العبارة[114]:
. ipconfig /all

سابعا: الاختيار السليم لشركات استضافة المواقع الالكترونية

حسن اختيار المستضيف له دور كبير في تجنب أضرار اختراقات المواقع[١١٥]، ففي العادة المستضيف يأخذا نسخا احتياطية يومية أو أسبوعية وشهرية ، حيث أن بعض شركات الاستضافة تأخذ نسخا أسبوعية ، فمثلا لو حدثت عملية اختراق في بداية الأسبوع أو نهايته ، فهذا يعني أن ملفات الأسبوع كامل انتهت ولا يمكن استرجاعها أو كل التحديثات التي أجريت خلال الأسبوع انتهت ، ويقع على المستضيف عبء إذا قصر في حفظ هذه الملفات ، لكن وحتى يتم إلزام المستضيف لابد من وضع ضوابط وتشريعات حتى يتقيد بها .

بدأت نسبة الجريمة الالكترونية بالارتفاع في المملكة الأردنية الهاشمية ، حيث وصل عدد جرائم أنظمة المعلومات المرتكبة في المملكة حتى نهاية شهر تشرين ثاني عام ٢٠١١ حوالي١١٠٣، بحسب إحصائيات الأمن العام[١١٦].

حيث أصبحت جرائم أنظمة المعلومات تنطوي على مخاطر جسيمة وتهدد بوقوع خسائر للمؤسسات والإفراد إضافة إلى أنها قد تهدد الأمن الوطني مما استدعى المشرع الأردني بالإسراع في إصدار قانون جرائم أنظمة المعلومات المؤقت لسنة ٢٠١٠ ، ويهدف هذا القانون إلى تحديد عناصر جرائم أنظمة المعلومات ومعالجة الثغرات والنقص التشريعي في التصدي للجرائم المستحدثة التي ترتكب باستخدام نظام المعلومات أو الشبكة المعلوماتية وبناء الثقة والأمان في استعمال تكنولوجيا المعلومات .

أمّا بالنسبة لجريمة الدخول الغير مشروع إلى موقع الكتروني أو نظام معلومات فقد أصبغ المشرع الأردني الحماية التشريعية لها في قانون جرائم أنظمة المعلومات لعام ٢٠١٠، ويستخدم الدخول غيرالمشروع لنظام المعلوماتي في الغالب كمرحلة سابقة وهامة لارتكاب جرائم أخرى كسرقة المعلومات أو تزويرها أو التجسس المعلوماتي أو جريمة الاحتيال المعلوماتي أو الاعتداء على حرمة الحياة الخاصة أو الترويج للدعارة أو تهديد الأمن الوطني أوغير ذلك من

---

(114) امن المعلومات ، المرجع السابق ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

(115) اختراق المواقع الالكترونية حال الأزمات: تشخيص وحلول بحث منشور على الانترنت:
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/50-internet-and-web-services-security/1192-hacking-websites-in-crisis-diagnosis-and-solutions.html ٢٠١١/١١/٤.

(116) موقع الاردنية للانباء http://www.alordonia.com/news/citizen/16328.html ٢٠١١/١٢/٣١

الجرائم وفي مثل هذه الحالات يشدد المشرع العقوبة وهو ما أخذ به المشرع الأردني في نصوص المواد (٤، ٥، ٦، ٧ ، ٨ ، ٩، ١٠، ١١) من قانون جرائم أنظمة المعلومات لعام ٢٠١٠[١١٧]، ورغم ذلك فقد يهدف مرتكب الفعل الدخول إلى النظام المعلوماتي ذاته دون أن يقصد ارتكاب جريمة أخرى ، وهو ما أشار اليه المشرع الأردني بنص المادة الثالثة/ا من قانون جرائم أنظمة المعلومات ، وقد يكون بهدف إتلاف المعلومات أو تعديلها بنص المادة ٣/ب وذلك بالنص القانوني التالي:

المادة٣- أ- كل من دخل قصداً موقعاً الكترونيا أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلنا هاتين العقوبتين .

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار أو بكلتا هاتين العقوبتين[١١٨].

الملاحظ على هذا النص القانوني أن المشرع الأردني في حقيقته يعاقب بموجبه على جريمتين الأولى هي الدخول المجرد غير المشروع إلى النظام محل الحماية وهو نظام المعالجة الآلية أي برامج الحاسب الآلي ،وأما الجريمة الثانية فهي جريمة الدخول غير المشروع بهدف تعديل المعطيات المخزنة أو إتلاف تشغيل النظام ِ، وقد يكون الدخول غير المشروع بهدف تحقيق نتيجة جرمية أخرى حسب نصوص المواد المشار إليها سابقا ، ولقد شدد فيه المشرع العقاب في الجريمة الثانية باعتبارها ظرفا مشددا، وضرورات البحث تقتضي أن يكون لكل جريمة فصلا مستقلا.

---

(117) قانــون جرائــم أنظمــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

(118) المادة الثالثة من قانــون جرائــم أنظمــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

الفصل الأول

جريمة الدخول المجرد غير المشروع إلى موقع الكتروني أو نظام معلومات

كان لصدور قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ والذي بدا العمل به ودخل حيز التنفيذ منتصف شهر آب من عام ٢٠١٠، بعد نشره في الجريدة الرسمية، الدافع الأكبر منا نحن القانونين العمل على توصيف أسماء الجرائم الالكترونية الواردة في هذا القانون استنادا لنصوص المواد تطبيقا و إعمالا لمبدأ الشرعية الجنائية :

"لاجريمة ولاعقوبة إلا بنص "[١١٩]، ومقتضي هذا المبدأ ، أنه لا يجوز تجريم فعل لم ينص القانون النافذ علي تجريمه صراحةً وقت وقوعه ، كما لايجوز توقيع عقوبة علي مرتكب الجريمة خلاف تلك المقررة قانوناً لها ، سواء من حيث نوعها أو مقدارها . فلا يكتسب الفعل أو الامتناع صفته الجرمية إلا بنص قانوني يحدد الجريمة في أركانها وعناصرها ، ويرصد لفاعلها الجزاء المقرر قانوناً أياً كانت صورته [١٢٠]. ، فإذا لم يكن هناك نص يبين جريمة ويحدد عقوبتها وجب علي القاضي أن يحكم بعدم المسئولية مهما كان الفعل في نظره خطيراً [١٢١] ، واستنادا لمبدأ الشرعية فقد أشارت المادة الثالثة/ا من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ لجريمة الدخول المجرد غير المشروع قصدا إلى موقع الكتروني أو نظام معلومات، لتكون موضوع دراستنا في هذا الفصل ، علما بأن غالبية التشريعات المقارنة الحديثة تعاقب على الدخول المجرد غير المشروع إلى نظام المعالجة الحاسوبي[١٢٢].

تنص المادة الثالثة من قانون جرائم أنظمة المعلومات لعام ٢٠١٠على: (أ- كل من دخل قصداً إلى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين.(ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء

---

(119) فرج صالح الهريش ، جرائم تلويث البيئة ، دراسة مقارنة ،الطبعة الاولى ١٩٩٨ ، ص٩٧

(120) سليمان عبد المنعم ، النظرية العامة لقانون العقوبات ، دار الجامعة الجديدة للنشر ، الطبعة الاولى١٩٩٨ ، ص٣

(121) محمد مؤنس محب الدين ، البيئة في القانون الجنائي ، مكتبة الانجلو مصريه ،١٩٩٥ ، ص١٧٤

(122) مدحت رمضان ، الحماية الجنائية لموقع الإنترنت ومحتوياته ، ورقة عمل مقدمة لندوة التجارة الإلكترونية المنعقدة في المعهد العالي للعلوم القانونية والقضائية – بدبي ، ١٠-١١ مايو ٢٠٠٤ ، ص٩؛ د. هدى قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت ، دار النهضة العربية ، ٢٠٠٠ ، ص١٠٠

أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار أو بكلتا هاتين العقوبتين) [١٢٣].

والعلة من وراء تجريم المشرع الأردني لجريمة الدخول المجرد غير المشروع لموقع الكتروني أو نظام معلومات هو منع اقتحام النظام الآلي لمعالجة المعلومات بحد ذاته، ذلك أن النظام المعلوماتي يحوي معلومات وبيانات لها قيمة مادية و معنوية لا تقل عن قيمة الوثائق والأموال والحقوق الأخرى المحمية بموجب التشريعات النافذة[124]، كما قد تحتوي على دراسات ومعلومات خاصة أو أنها تتحكم بأنظمة أو مؤسسات وتسيرها.

وسوف نعالج هذه الجريمة (جريمة الدخول المجرد غير المشروع عن قصد إلى موقع الكتروني أو نظام معلومات) في هذا الفصل ضمن مبحثين:

المبحث الأول : تجريم الدخول غير المشروع لنظام معلومات أو موقع الكتروني.

والمبحث الثاني: أركان جريمة الدخول المجردغير المشروع لنظام معلومات أوموقع الكتروني.

المبحث الأول :تجريم الدخول المجرد غير المشروع لنظام معلومات أو موقع الكتروني

نعالج في هذا المبحث ماهية الدخول المجرد غير المشروع لنظام معلومات أو موقع الكتروني وحمايتها (كمطلب أول) والطبيعة القانونية لجريمة الدخول المجرد غير المشروع (كمطلب ثاني).

---

[123] المادة الثالثة من قانــون جرائــم أنظمــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

[124] شيماء عبد الغني محمد عطا الله مكافحة جرائم المعلوماتية في المملكة العربية السعودية بحث منشور http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx#_ftn4: 21/11/2011

المطلب الأول: ماهية الدخول المجرد غير المشروع لنظام معلومات أو موقع الكتروني وحمايتها

ويقصد بالدخول إلى النظام بشكل عام جميع الأفعال التي تسمح بالولوج إلى نظام المعلومات والاحاطه والسيطرة على المعطيات التي يتكون منها(١٢٥) .

لا يقصد بالدخول هنا الدخول بالمعنى المادي،أي الدخول إلى مكان أو منزل أو حديقة، إنما يجب أن ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نتحدث عن الدخول إلى ملكة التفكير لدى الإنسان،أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، ولم يحدد المشرع الأردني وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة ،و يستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر(عن طريق الاعتراض غير المشروع لعمليات الاتصال)(١٢٦).

والدخول هنا يتحقق من خلال إجراء الاتصال بالنظام بأي طريقة من الطرق ، فالدخول من الممكن أن يتحقق سواء استخدم الشخص قرصا أو جهاز تلفونيا أو حاسوب آخر موجود على الشبكة أو قام بضرب حروف الرقم السري الذي يحمي البرنامج(١٢٧) ، وسوف نعالج في هذا المطلب تعريف الدخول غير المشروع لنظام معلومات (كفرع أول) وحماية النظم الأمنية (كفرع ثاني).

الفرع الأول : تعريف الدخول غير المشروع لنظام معلومات

الدخول غير المشروع يقصد به الدخول إلى نظام معلومات أو إلى موقع الكتروني من قبل شخص غير مخوّل له بالدخول ، فينتهز الفاعل هذه الفرصة للإطلاع على ملفات أخرى سرية دون وجه حق(١٢٨)، ويعد الدخول غير مشروع متى كان ذلك مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه، ومن الأمثلة على ذلك تلك الأنشطة المتعلقة بأسرار الدولة أو التي تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة ولا يجوز الاطلاع عليها (١٢٩) .

---

(125) نائله قوره ، جرائم الحاسب الاقتصادية ، دار النهضة العربية ، القاهره، الطبعة الاولى ، ٢٠٠٤، ص٣٤٣ ، وانظرد. عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الكتب القانونية- مصر، ط١ ٢٠٠٧، ص ٣٥٣ وما بعدها

(126) فشار عطاء الله ، مواجهة الجريمة المعلوماتية في التشريع الجزائري ،بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية تم عقده بأكاديمية الدراسات العليا بليبيا فى أكتوبر ٢٠٠٩ ، وانظر نائله قوره ، المرجع السابق ، ص٣٢٥

(127) عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الالي وابعادها الدولية ، دار النهضة-القاهره ، ١٩٩٥، الطبعة الاولى ، ص ١٢٧ و د.محمد حمّاد الهيتي ، مرجع سابق ، ص١٨٢

(128) الدكتورة شيماء عبدالغني محمد عطاالله مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، بحث منشور على: 21/11/2011http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx#_ftn4:

(129) عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية: الكتاب الثاني، الحماية الجنائية للتجارة الالكترونية، دار الفكر الجامعي الإسكندرية ٢٠٠٢، ص ٢٤

و الدخول غير المشروع يشمل كل استعمال للحاسب الآلي دون رضاء صاحب الحق ، أيا كانت صورة ذلك الاستعمال[١٣٠] ، كما لو تمكن الفاعل من تشغيله مباشرة أو عن بعد[١٣١] .

ولا يشترط أن يكون النظام الحاسوبي محميا بكلمة السر، بل إن الدخول غير المشروع معاقب عليه حتى ولو لم يخصص صاحبه كلمة مرور لكي يحميه من تطفل الآخرين[١٣٢]. والمشرع الأردني تبنى هذا الاتجاه بحماية الحاسب الآلي دون اشتراط أن يكون النظام الآلي محميا بكلمة مرور.

والدخول إلى النظام المعلوماتي لا يشكل جريمة بحد ذاتها إلا في الأحوال التي يكون الدخول قد تم بدون وجه حق ، وبالتالي فإنه لا يعد دخولا غير مشروع إذا توافر رضاء صاحب النظام كأن يكون هنالك اتفاق بينهما أو كان الجهازان ينتميان إلى شبكة واحدة و متصلان بالشبكة ذاتها مما يفيد توافر الرضاء الضمني بدخول العاملين على الجهاز الخادم للشبكة إلى الأجهزة المنتمية إلى ذات الشبكة[١٣٣] .

ومن التطبيقات على ذلك شبكة الجامعة الأردنية التي تهيمن على أجهزة العاملين بها ،الموجودة في مكاتب كليات الجامعة وإداراتها ومراكزها المختلفة، ولما كانت تلك الأجهزة تنتمي إلى العمل أي أنها من أدوات العمل، فلكل من العاملين المصرح لهم بالدخول الحق في الدخول إلى تلك الأجهزة والاطلاع على الملفات الموجودة بها، ولا يعتبر ذلك من قبيل الدخول غير المشروع.

كما لا يعد من قبيل الدخول غير المشروع أن يتم ذلك من جهة عامة لها الحق في مراقبة أجهزة الحاسب الآلي المتواجدة لدى الأفراد إذا كان المشرع يسمح لتلك الجهات بممارسة الحق في المراقبة.

وقد حدد المشرع الأردني الدخول غير المشروع في المادة الثالثة من قانون جرائم أنظمة المعلومات بثلاث حالات (أ- كل من دخل قصداً إلى موقعٍ الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ..)

الصورة الأولى : الدخول دون تصريح.

الصورة الثانية : الدخول بما يجاوز التصريح.

---

(130)عبد الفتاح بيومي حجازي، المرجع السابق، ص ٢٤

(131) جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب الآلي) ، دار النهضة العربية، ١٩٩٢، ص ٦٦

(132) محمد سامي الشوا ، المرجع السابق ، ص36

(133) شيماء عبدالغني محمد عطاالله مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، بحث منشور على: 21/11/2011http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx#_ftn4:

الصورة الثالثة : الدخول بما يخالف التصريح.

أولا : الصورة الأولى الدخول دون تصريح

ويعرف التصريح كما أورده المشرع الأردني في نص قانـــون جرائـــم أنظمـــة المعلومات(بأنه الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع الكتروني أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع الكتروني أو إلغائه أو تعديل محتوياته) [١٣٤].

ويعرف الدخول غير المصرح به كذلك بأنه:الوصول أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن[١٣٥].

بمعنى آخر يكون الدخول غير مصرح به عندما يقوم الفاعل بالدخول إلى النظام المعلوماتي دون موافقة المسئول عن النظام أو مالكه ،ويرتبط هذا المفهوم أساسا بمعرفة من له الحق أو السلطة في الدخول إلى النظام .ومناط عدم المشروعية يكمن بانعدام سلطة الفاعل في الدخول إلى النظام مع علمه بذلك وعليه فان مجرد الدخول إلى نظام الحاسب الآلي لا يشكل فعلا غير مشروع وإنما تتوافر فيه عدم المشروعية من زاوية عدم الصلاحية بمعنى أن هذا الدخول يتم دون وجه حق.

ثانيا: الصورة الثانية بما تجاوزالتصريح

إذا كان دخول الفاعل لديه تصريح بالدخول إلا أنه تجاوز الصلاحيات الممنوحة له [١٣٦]،كأن يسمح له باستخدام نظام المعلومات أو الشبكة المعلوماتية لمدة معينة ولكنه بقي يشغلها مدة إضافية [١٣٧].

المشرع الأردني اعتبر تجاوز التصريح (جريمة الإبقاء على الاتصال أو المكوث فيه) إحدى صور الدخول غير المشروع حيث أشار إليها المشرع الأردني في نفس الماد 3/ا(– أ– كل من دخل قصداً إلى موقعٍ الكترونيٍ أو نظام معلومات بأي وسيلة دون ..... أو يجاوز التصريح..).

---

(134)المادة الثانية من قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

(135)عبد الفتاح مراد ، المرجع السابق، ص ٢٤١

(136) صالح احمد يوسف ، الدخول غير المشروع على الانظمة المعلوماتية ، مقال منشور على الرابط http://irbd.hooxs.com/t16012-topic 19/11/2011

(137) كما أشارت المذكرة الايضاحية لقانون جرائم أنظمة المعلومات http://www.slideshare.net/UrdunMubdi3/31-72010-2 18/11/2011

بينما نلاحظ أن المشرع الفرنسي اعتبر تجاوز التصريح جريمة مستقلة وهي جريمة الإبقاء على الاتصال أو المكوث فيه بعد حصوله وقد عبر عن ذلك المشرع الفرنسي في المادة ٣٢٣-١ من قانون العقوبات الفرنسي جرّمت البقاء غير المصرح بهما داخل كل أو جزء من نظام المعالجة الآلية للمعلومات. [١٣٨]

ويمكن القول إن جريمة الإبقاء على الاتصال هي من طائفة جرائم الامتناع التي تتحقق بالفعل الايجابي إذ أنها في الوقت الذي يلقي المشرع على الشخص واجب الامتناع عن البقاء في النظام يتطلب منه القيام بعمل هو قطع الاتصال (عدم الإبقاء عليه).

ويمكن التمييز بين طائفتين تنطبق عليهما بصفة عامة صفة الدخول غير المشروع (صورة بما تجاوز التصريح) إلى أنظمة الحاسب الآلي أولا الأشخاص من داخل المؤسسة المسئولة عن النظام المؤسسة، والأشخاص من خارج المؤسسة ، فالنسبة إلى الدخول غير المشروع إلى النظام والذي يتم من قبل الفئة الثانية فلا يوجد ثمة مشكلة لان دخولهم يكون من خارج نطاق شبكة العاملين الذين يتنمون لنفس مجموعة العمل ، وإنما المشكلة تثور في حالة لو تم الدخول من قبل الطائفة الأولى وهم العاملون بالمؤسسة التي يوجد بها النظام ففي هذه الحالة بتجاوز العامل السلطة الممنوحة له ، ويصعب في كثير من الأحيان معرفة عما إذا كان التجاوز قد تم عمدا أو عن طريق الخطأ [١٣٩].

ثالثا: الصورة الثالثة بما يخالف التصريح

كذلك أثار تحديد مفهوم عدم التصريح بالدخول إلى أنظمة الحاسبات الآلية تساؤلا آخر يتعلق بالحالة التي يكون الدخول إلى النظام مصرحا به ،إلا أنه يستخدم لغرض آخر غير الغرض الأصلي المصرح به ، كأن يكون مسموحا له الوصول لبعض المعلومات في الشبكة الداخلية ولكنه خالف ذلك ودخل قصدا إلى قسم آخر من تلك الشبكة كنظام الموظفين أو بريدهم فمجرد الوصول لنظام أو شبكة محمية يشبه الدخول إلى منزل خاص بالغير ليس متاحا للعموم دون إذن صاحبه ولا حاجة أن يكون الدخول بغرض السرقة فقد يكون الدخول لمجرد إثبات المقدرة على تجاوز ومخالفة التصريح[١٤٠].

---

[138] محمد حمّاد الهيتي، مرجع سابق ، ص١٩٠

[139] صالح احمد يوسف ، الدخول غير المشروع على الانظمة المعلوماتية ، مقال منشور على الرابط http://irbd.hooxs.com/t16012-topic 19/11/2011

[140] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات http://www.slideshare.net/UrdunMubdi3/31-72010-2 18/11/2011

في الحقيقة أن الدخول إلى نظام الحاسب الآلي لابد وأن يكون مقيدا بالغرض الذي أعطيت من أجله هذه السلطة ، فعندما يتعارض غرض الدخول إلى النظام مع الغرض الأصلي أصبح غير مشروع وبالتالي تقوم به جريمة الدخول غير المشروع .

الفرع الثاني : حماية النظم الأمنية

يقصد بالنظم الأمنية : القواعد الأمنية التي تتخذ لحماية نظم الحاسبات الآلية في مواجهة الأخطار المختلفة سواء أكانت أخطار مادية ناشئة عن الكوارث الطبيعية أو نقص في التيار الكهربائي أو أخطار ناشئة عن أخطاء بشرية أو أفعال إجرامية مختلفة التي تتصل بالحاسبات الآلية[١٤١].

وعليه تنوع المخاطر التي تتعرض لها تقنية المعلومات ومنها : المخاطر الطبيعة ،المخاطر العامة والمخاطر الالكترونية.

أولا :المخاطر الطبيعية والعامة

يقصد بالمخاطر الطبيعية الكوارث الطبيعية والحريق والزلازل وما شابه ، أما المخاطر العامة تتنوع ما بين انقطاع التيار الكهربائي وانقطاع الانترنت وسرقة البيانات المحفوظة على الأقراص الصلبة ،ويمكن القول انه يمكن التعامل مع المخاطر الطبيعية والعامة من خلال توفير وسائل وإجراءات الحماية لأجهزة الكمبيوتر والشبكات والبنية التحتية ، كاستخدام مفاتيح الأبواب الذكية للوصول إلى الأجهزة واستخدامها من المخولين بذلك فقط [١٤٢].

ثانيا : المخاطر الالكترونية

وهنا نعني المخاطر التي قد تحدث للمعلومات داخل النطاق الإلكتروني،مثل تلك المعلومات المخزنة في الحاسب الشخصيclient مرورا بالشبكة حتى جهاز الخادم server.

وتتضمن تلك المخاطر أساليب مختلفة، فهناك انتحال الشخصية، والاستخدام الغير المصرح له، وعرقلة الخدمة، والتصنت والاقتحام، ولا ننسى أكثر المخاطر إمعانا في الشر هي عمل ونشر الفيروسات[١٤٣] وديدان الانترنت[١٤٤] .

---

(141) مصطفى فتحي خطاب، ورشةعمل (تطبيقات عملية فى أمن المعلومات) المنظمة العربية للتنمية الادارية - القاهرة ، عقدت بتاريخ٢٠١٠/٦/٢٤ unpan1.un.org/intradoc/groups/public/.../arado/unpan024009.pps، ٢٠١١/١١/٢٠

(142) مصطفى فتحي خطاب، ورشةعمل (تطبيقات عملية فى أمن المعلومات) المنظمة العربية للتنمية الادارية - القاهرة ، عقدت بتاريخ٢٠١٠/٦/٢٤ unpan1.un.org/intradoc/groups/public/.../arado/unpan024009.pps، ٢٠١١/١١/٢٠

(143) هو برنامج صغير مكتوب باحد لغات الحاسوب ويقوم باحداث اضرار في الحاسب والمعلومات الموجودة فيه ويقوم بنسخ نفسه على الملفات الموجودة في الحاسب

(144) اهمية امن المعلومات ، مقال منشور http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/54-assurance-awareness-education-and-training/801-importance-of-information-security.html ٢٠١١/١١/١٤

إلا أنه ونظرا لما لهذا الفعل من آثار سلبية ومخاطر عديدة سواء على الأنظمة ذاتها أو على المعطيات المخزنة بداخله وللخسائر المادية التي تترتب على فعل الدخول ذاته أو التي قد تترتب على محاولة وقفه .مما دفع بالقائمين على حفظ المعلومات والبيانات إلى اتخاذ إجراءات تتدرج فيما بينها من حيث درجة التعقيد التي تتميز بها حيث تبدأ بقواعد الأمن المادية التي تتمثل في حماية الحاسبات الآلية بوضعها في أماكن تكفل لها أن تكون بعيدة عن أية أعمال تهددها ، وهناك بعض القواعد الأكثر تعقيدا تتمثل في وضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من تلك الأجهزة ، ومن بينها أيضا استخدام أسلوب توزيع العمليات التي يقوم بها النظام الحاسب الآلي ونقلها إلى نظام احتياطي Back - up ، أيضا من بين تلك القواعد استخدام الاختبارات الفيزيولوجية (الوظائفية) للدخول إلى النظام وذلك عن طريق التحقق من شخصية القائم بعملية الدخول عن طريق بصمة الإصبع – البصمة الإلكترونية أو نبرة الصوت أو شكل الأذن[١٤٥] ، وهناك أسلوب التشفير لحماية المعلومات.

المطلب الثاني : الطبيعة القانونية لجريمة الدخول غير المشروع لنظام معلومات

يقسّم الفقه الجرائم إلى نوعين جرائم مادية (ضرر) ، وجرائم شكلية (خطر) [١٤٦] . وهذا يثير التساؤل التالي : ما هي طبيعة جريمة الدخول غير المشروع إلى أنظمة الحاسبات ،هل تعد جريمة ضرر أم جريمة خطر؟ بمعنى أخر هل يجب أن يكون الدخول غير المشروع منتجا لأثرا ما ، أي يؤدي إلى نتيجة إجرامية محددة كالوصول إلى المعطيات المختلفة التي يحتويها هذا النظام أم إن الجريمة تتم بمجرد الدخول ؟

الواضح من النص القانوني[١٤٧] أن الدخول غير المشروع المجرم حسب النص هو الدخول المجرد ، حيث أن الجريمة تقوم بمجرد الولوج إلى النظام مادام أنه لا يلزم لوقوعها تحقق ضرر من نوع معين[١٤٨] ،طالما أن الدخول كان بدون وجه حق . وعليه تعتبر جريمة الدخول غير المشروع إلى نظام معلومات من الجرائم الشكلية التي لا يستلزم لتحققها تحقق نتيجة معنية [١٤٩]

---

(145) السمات الحيوية – البصمة الصوتية ، مقال منشور على موقع مركز التميز لامن المعلومات الرابط: http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/53-smart-card-and-biometrics-security/1495-vital-features-voice-tag.html ٢٠١١/١١/١٣

(146) الجرائم تقسم إلى نوعين جرائم مادية (ضرر) وهي الجرائم ذات نتيجة ، وجرائم شكلية(خطر) ويقصد بها الجرائم ذات سلوك ونشاط بحت ،د. محمد سامي النبراوي ، شرح الاحكام لقانون العقوبات الليبي ، منشورات جامعة قار ،١٩٨٧، الطبعة الثالثة ، ص ١١٨

(147)المادة الثانية من قانــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

(148) محمد حمّاد الهيتي ، مرجع سابق ،صفحة ١٨٧

(149)جميل عبد الباقي الصغير، المرجع السابق، صفحه ١٥٠ .

، و الركن المادي للجريمة الشكلية يكتمل بالنشاط الايجابي الذي يصدر من الجاني دون تطلب تتحقق نتيجة مادية منفصلة عنها [١٥٠].

وبذلك نلاحظ أن التشريعات الحديثة اتجهت إلى تجريم جرائم الخطر بعد أن كانت تكتفي بتجريم جرائم الضرر ، وترمي التشريعات الحديثة من خلال هذا التجريم إلى حماية المصالح القانونية ، وهي حماية ضرورية في العصر الحالي ، إذ أسفر التطور الثقافي والاجتماعي عن ظهور أوضاع متعددة ينشأ عنها تهديد للمصالح القانونية[١٥١] .

وهو ما اخذ به المشرع الأردني عندما عالج جريمة الدخول غير المشروع لموقع الكتروني اونظام معلومات [١٥٢].

ويبرر الفقه هذا النهج [١٥٣] الذي أخذت به التشريعات الحديثة وخصوصا التشريعات الخاصة بأنه لا مناص من تجريم الخطورة الناتجة عن بعض الأنشطة التي تدور في محيط الحياة المعاصرة مثلما هو في محيط الحياة الاقتصادية[١٥٤] ومحيط حماية أنظمة المعلومات والمواقع الالكترونية ،نظراً لما تتسم به هذه المجالات من تعقيد وتكتيك متتابع سريع الخطي ، وهو ما يفسر تعاظم جرائم الخطر في مواجهتها لأنشطة لا يمكن أو يصعب تقييم آثارها وإن أمكن تقييمها بمعيار المخاطرة. والخطر هو صلاحية عامل معين أو ظروف ما لإحداث ضرر ما ([١٥٥])،

وهنا نشير هو عدم تصور الشروع في الجرائم الشكلية وتصوره في الجرائم المادية ذلك لان الشروع يعني تخلف النتيجة الجرمية بسبب لا دخل لإرادة الفاعل في ذلك[١٥٦] .

ومع أن هذه الجريمة من الجرائم الشكلية التي لا يتطلب المشرع تحقق نتيجة معينة وفقا لمدلولها المادي فيها إلا أن المتصور أن يترتب على ارتكابها إحداث ا ضرار لا تدخل في تكوينها أي انه من الممكن أن يترتب على الدخول إلى النظام العبث بالبرامج التي يعمل بها أو بالمعلومات التي يختزنها مما يحدث أضرار بالبرنامج سواء بمحو تلك البيانات أو المعلومات أو البرامج أو حتى بتعديلها[١٥٧].

([150]) للنتيجة مدلاولان مادي ومعنوي ، والاول يعني التغيير الناتج عن السلوك الاجرامي في العالم الخارجي ، والثاني يمتثل بالعدوان الذي ينال مصلحة او حقا يحميه القانون. د. علي حسين الخلف ، الاحكام العامة في قانون العقوبات ، دار الرسالة –الكويت ١٩٨٢، ص ١٠٤

([151]) د.سليمان عبد المنعم ، المرجع السابق ، ص١٨

([152]) المادة الثانية من قانــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

([153])عمر السعيد رمضان ، شرح قانون العقوبات القسم العام ،دار النهضة العربية –القاهره ،١٩٩٨، الطبعة الاولى ، ص١٦٢

([154])نور الدين هنداوي ، الحماية الجنائية للبيئة ، دراسة مقارنة ، دار النهضة العربية -القاهره، ١٩٨٥ ، ط١، ص٣٥ .

([155]) محمد مؤنس محب الدين ، المرجع السابق ،ص١٩٥

([156]) محمد حمّاد الهيتي ، مرجع سابق ،صفحة ١٨٨

([157]) محمد حمّاد الهيتي ، مرجع سابق ،صفحة ١٨٨

والى جانب كون جريمة الدخول غير المشروع جريمة شكلية ، فان بعض الفقه [١٥٨] اعتبرها من ضمن طائفة الجرائم المستمرة معللا ذلك بان سلوك الجاني في هذه الجريمة يمتد طالما ظل يشغل النظام المعلوماتي بطريق غير مشروع[١٥٩] والبعض الآخر من الفقه اعتبرها من الجرائم الوقتية [١٦٠]، حيث أن هذه الجريمة تتحقق بمجرد فعل الدخول غير المصرح به[١٦١]، ونحن نؤيد مع ذهب إليه الاتجاه الأخير لان هذه الجريمة تتحقق بالدخول المجرد غير المشروع دون أن تتطلب تحقق نتيجة جرميه لنظام المعلومات بدلالة نص المادة ٣/ا من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ .

والمقصود بالجريمة الوقتية هي التي يقع وينتهي نشاطها الجرمي في لحظة زمنية قصيرة دون ان يكون ذلك التنفيذ قابلا للامتداد في الزمن إلى ما بعد هذه اللحظة ومن أمثلتها القتل والقدح والتحقير لأنها تقع وتنتهي بوقوع السلوك الذي يقوم به الركن المادي المادي للجريمة[١٦٢]، بينما تعرف الجريمة المستمرة: على أنها تلك الجريمة التي يستغرق تحقيق نشاطها الجرمي زمنا طويلا نسبيا مثل حمل سلاح دون ترخيص [١٦٣].

ولتحديد ما إذا كانت الجريمة مستمرة أو وقتية فانه يتعين الرجوع إلى نص القانون الخاص بالجريمة لاستخلاص عناصرها وتحقق ما إذا كانت تستغرق زمنا قصيرا أو طويلا ولكن الصعوبة تبدو في تحديد الضابط بين الزمن الطويل والزمن القصير[١٦٤] ولكن كما يقول بعض الفقه [١٦٥] أن الضابط في تمييز بين زمن طويل والزمن القصير متروك لتقدير قاضي الموضوع من خلال الاستعانة بالظروف التي أحاطت بتنفيذ الجريمة ويعتبر معيار الزمن للتمييز بين الجرائم الوقتية والمستمرة هو ضابط نسبي .

وتكمن أهمية التفرقة بين الجرائم الوقتية و الجرائم المستمرة في جانبين أولا:من جهة الاختلاف في تطبيق أحكام قانون العقوبات سواء من ناحية السريان الزماني لنصوص العقوبات و السريان

([158]) جميل عبد الباقي الصغير، المرجع السابق، صفحه ١٥٠

[159]د.محمد حمّاد الهيتي ، المرجع السابق ،صفحة١٨٨

([160]) سامي حمدان الرواشده/د.أحمد موسى الهياجنه، مكافحة الجريمة المعلوماتية بالتجريم والعقاب : القانون الانجليزي نموذجا، بحث منشور في المجلة الاردنية في القانون والعلوم السياسية ، المجلد(١) العدد(٣) تشرين الاول ٢٠٠٩ ص١٣٧

([161]) نهلا المومني ، الجريمة المعلوماتية في قانون العقوبات الاردني ،جرائم الحاسوب والانترنت، رسالة ماجستير الجامعة الاردنية ٢٠٠٥، ص١٢٤

([162]) كامل السعيد ، المرجع السابق، ص٢٢٥

([163]) علي حسين الخلف ، سلطان الشاوي ، الاحكام العامة في قانون العقوبات ، دار الرسالة –الكويت ، بدون طبعة ، ١٩٨٢، ص ٣١٤ ، د. محمد سامي النبراوي ، مرجع سابق ص ٤٥،ا.د.كامل السعيد ،مرجع سابق ، صفحة ٢٢٥و٢٢٦

([164]) نظام توفيق المجالي صفحة، شرح قانون العقوبات القسم العام، دار الثقافة للنشر والتوزيع -عمان، ط١، ٥٤و٥٥

([165]) محمود نجيب حسني ، المرجع السابق، صفحه ٣٢١

المكاني لهذه النصوص ومن ناحية أخرى تبدو لهذه التفرقة أهمية في تطبيق أحكام قانون أصول المحكمات الجزائية سواء من جهة الاختصاص الإقليمي و تقادم الدعوة الجزائية ومن حيث قوة الشيء المحكوم فيه(١٦٦) .

المبحث الثاني :أركان جريمة الدخول المجرد غير المشروع لنظام معلومات أو موقع الكتروني

تقوم الجريمة حسب الرأي الغالب(١٦٧) في الفقه على ركنين مادي ومعنوي ، إذ انه من المبادئ المستقرة في القانون الجنائي إن كل جريمة يتطلب لقيامهما تحقق ركن مادي ويتمثل بواقعه تسبب ضررا أو تشكل خطرا على المصالح المحمية قانونا، تنسب إلى مسببها وتسند إليه من الناحية المادية تبعا لنوع الرابطة السببية التي تقرر صلة النتائج بالأفعال وتكون ثمة صلة نفسية تعكس الموقف النفسي بين الفعل ونفسية محدثه .

وجريمة الدخول غير المشروع تقوم كسائر الجرائم الأخرى على ركنين:الركن المادي يتمثل بنشاط أو سلوك إجرامي الذي يحقق الدخول غير مشروع إلى النظام المعلوماتي والركن الثاني المعنوي الذي يتمثل بالقصد الجنائي وخصصنا لكل منهما مطلبا مستقلا وأخيرا موقف التشريعات المقارنة التي أخذت بتجريم الدخول المجرد غير المشروع لنظام معلومات كمطلب ثالث.

المطلب الأول الركن المادي المكون لجريمة الدخول غير المشروع نظام معلومات

تتحقق الجريمة من ركن مادي لا بد من توافره وبدونه لا يتصور قيامها، وبالتالي لاتجوز كقاعدة عامة المعاقبة بدون القيام به (١٦٨) ويقصد بالركن المادي للجريمة أو الواقعة الجرمية سلوك

---

(166) نظام توفيق المجالي ، المرجع السابق ، صفحة ٥٤و٥٥

(167) لان هناك من الفقهاء من يذهب الى اضافة ركن آخر للجريمة يصطلح عليه بالركن الشرعي ، انظر د. علي حسين الخلف، سلطان الشاوي ، المرجع السابق، ص١٣٨

(168) كامل السعيد ،مرجع سابق، صفحة١٠٨

اجرامي يتمثل بارتكاب فعل جرمه القانون، أو الامتناع عن فعل أمر به القانون[١٦٩]، ومن خلال استقراء نص المادة الثالثة/ا من قانون أنظمة المعلومات لعام (٢٠١٠) ، فان الركن المادي فيها يتكون من عنصر واحد وهو النشاط المتمثل في الدخول غير المشروع عن قصد إلى موقع الكتروني أو نظام معلومات دون أن يتطلب تتحقق نتيجة مادية لهذا الدخول غير المشروع.

الواضح من النص السابق أن الدخول غير المشروع المجرم هو الدخول المجرد وهو محل الجريمة، حيث أن الجريمة تقوم بمجرد الولوج إلى النظام حتى وإن لم يترتب على فعل الدخول نتيجة جرميه ،و يكفي لوقوع النشاط المعاقب عليه أن يقوم المتهم بالدخول إلى نظام المعلومات بطريقة غير مشروعه حتى لو كان الدخول عن بعد إلى النظام، وحتى ولو كانت الملفات محمية بكلمة المرور ولم يتمكن من فتحها[170].

فالأمر في تجريم الدخول ليس تجريما ماديا بل هو تجريم معنوي. فالفاعل لا يقوم بالدخول إلى النظام بالكسر أو باستعمال مفاتيح مصطنعة، بل يمكن أن يتم ذلك من على بعد باستعمال برامج الهاكر أو بغيره من الوسائل ، وخلاصة القول أن هذه الجريمة يقوم ركنها المادي على فعل الدخول غير المشروع فقط (الاختراق) والذي يمثل النشاط الجرمي لجريمة الدخول غير المشروع ويتحقق الاختراق بوسائل وطرق متنوعة[171] ،وتختلف الوسائل التي يمكن اللجوء إليها من أجل الدخول غير المشروع إلى تلك الأنظمة ، إلا أنها جميعها تفترض قدرا من المعرفة بتكنولوجيا الحاسبات الآلية [١٧٢].

ويعرّف الدخول غير المشروع بالاختراق أوالنشاط الذي يقوم به الجاني لدخول الموقع الالكتروني أو نظام المعلومات ،و قد يكون مباشرا وقد يكون غير مباشر (مبطن) وخصصنا لكل محور منهما فرعا مستقلا .

الفرع الأول : الاختراق المباشر للشبكات وأنظمة المعلومات

يعتمد هذا النوع من الدخول غير المشروع على استغلال المنافذ المفتوحة بنظم التشغيل أو برامج الحماية ، التي هي في الأساس أخطاء برمجية بشرية ، ويقع تحته مجموعة من الأساليب منها:

---

(169) المادة٢٨ من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩

(170) شيماء عبدالغني محمد عطاالله مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، منشور على 21/11/2011http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx#_ftn4:

(171) شيماء عبدالغني محمد عطاالله مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، بحث منشور على الرابط التالي 21/11/2011http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx#_ftn4:

(172) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، بحث منشور على 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

أولا.البحث عن المنافذ المفتوحة عن طريق الشبكات

يتطلب الاختراق المباشر الكثير من الجهد والمثابرة وتكرار المحاولة لاكتشاف المنافذ المفتوحة والدخول منها إلى الجهاز ، فبعد تحديد الهدف المراد اختراقه « بريد إلكتروني أو موقع أو شبكة محلية مرتبطة بالإنترنت »[١٧٣] يحتاج المخترق إلى جمع اكبر قدر ممكن من المعلومات حول مظاهر أمن النظم الخاصة بالهدف المراد اختراقه قبل القيام بعملية الاختراق ، وتشمل عملية جمع المعلومات أسماء الميادين وكتل الشبكات وعناوين IP[١٧٤] وخدمات TCP[175] وخدمات TCP/UDPوبنية النظام ، وأسماء المستخدمين والمجموعات ، وبروتوكولات الشبكة المستخدمة ، وأرقام الهواتف الرقمية المستخدمة وآليات التحقق من صحة المعلومات. ويستطيع المخترق الحصول على المعلومات السابقة من خلال الصفحة الرئيسية أو البداية Home Bageالخاصة بالهدف حيث تعمد بعض المؤسسات إلى سرد الكثير من إعدادات الأمن الخاصة بها مباشرة على ملقم الإنترنت الخاص بها ، بالإضافة إلى بعض المعلومات الأخرى ، كالأماكن والمؤسسات أو العناصر المرتبطة كأخبار الدمج والتحصيل ، وأرقام الهواتف ، وأسماء المستخدمين وعناوين البريد الإلكتروني وسياسات الأمن والخصوصية التي تشير إلى أنواع آليات الأمن الموضوعة ، وارتباطه بملقم ويب آخر مرتبط بالمؤسسة . كما أن الحصول على نسخة من الموقع قد تسمح للمخترق بالبحث برمجيا وتجعل بذلك عملية جمع المعلومات أكثر فاعلية. كما تقدم مقالات الأخبار وإصدارات الصحف وغيرها دلائل إضافية حول وضع المؤسسة ، ومخطط الأمن بها[١٧٦].

كما قد يلجأ المخترق إلى استخدام عملية تعداد الشبكة(رقم الاي بي) في التعرف على أسماء المواقع حيث تمثل هذه الأخيرة حضور المؤسسة على شبكة الإنترنت . وهى المكافئ على الإنترنت لاسم المؤسسة ، ولكي يتم هذا التعداد يتم البدء باكتشاف الشبكات المقترنة بها ، وتساعد قواعد بيانات Who is المتعددة في تقديم ثروة من المعلومات المستهدفة ، كما توجد آليات مختلفة عديدة للاستعلام من قواعد البيانات

---

(173) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، بحث منشور على 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

(174) برتوكول IP هو البرتوكول الأساسي في مجموعة البروتوكولات المسئولة عن نقل حزم(packets) من مكان لآخر، انظر حسن طاهر داود، امن شبكات الحاسوب ، مكتبة الملك فهد الوطنية ، ٢٠٠٤ ، صفحه ٦٧

(175) برتوكول Tcp يستخدم مع برتوكول IP ومهمته التأكد من حزم ال (packets) قد وصلت الى وجهتها بالشكل الذي يسمح باعادة ترتيبها ، انظر حسن طاهر داود ، مرجع سابق صفحه٦٧

(176) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

ثانيا.مسح المنافذ:Port Scanning

وهو عبارة عن محاولة إجراء اتصال شبكي بالعديد من المنافذ على جهاز الحاسب الآلي المستهدف بغرض كشف نوع الخدمات الشبكية التي تعمل عليه ، ونظام التشغيل الخاص به ، أو تطبيقات معينة ذات ثغرات أمنية معروفة ليتم استغلال بعض المنافذ التي تكون في حالة استماع Listeningفي محاولة الاعتداء على هذا الحاسوب ، إما بالاختراق أو التعطيل عن العمل(177).

ويهدف هذا الأسلوب إلى مسح أكبر عدد ممكن من المنافذ في الحاسوب الواحد أو منافذ محددة في حواسيب تقع ضمن نطاق شبكة واحدة أو عدة شبكات وكشف نقاط الضعف في كل جهاز ، حتى أن بعض الأدوات المخصصة للقيام بذلك تحتوى على قاعدة بيانات بالأساليب الشائعة الاستخدام لاستغلال كل نقطة ضعف.

وهناك طرق كثيرة لاستخدام هذا الأسلوب ، تتفاوت قليلا من الناحية التقنية ، ولكل منها استخداماته خاصة ،مثل المسح التزامني الخفي(١٧٨)Stealth SYN Scan، والمسح الساكن Idle Scanning، وأسلوب الطعم الخادع (١٧٩)Spoofing Decoys ، وغير ذلك من طرق استخدام هذا الأسلوب.

وهناك العديد من الأدوات البرمجية المصممة للقيام بهذه المهمة وأكثرها مجاني ومتاح على شبكة الإنترنت منها على سبيل المثال Super Scanner , Win Scanوتعمل في بيئة الويندوز وكذلك Netcat , nmap لبيئة يونيكس(180.).

ثالثا. استغلال المنافذ المفتوحة:

عندما يتم الاتصال بالشبكات المحلية أو الدولية يصبح الجهاز أو النظام المعلوماتى بما فيه عرضة للاختراق ، ويتم ذلك باستغلال المنافذ الموجودة بالنظام أو برامج الحماية وذلك لأجل الدخول إلى الجهاز أو الشبكة المرتبطة بها. ومن المنافذ التي يمكن استغلالها تلك الموجودة في البرامج التي تعتمد نظام الزبون /الخادم Client/Server أو استغلال الفجوة الأمنية الموجودة في برامج الدردشة كبرنامج ICQ وهو أحد منتجات شركة Mirabils الإسرائيلية حيث يستخدم هذا البرنامج

---

(177) الدخول غير المشروع على انظمة انظمة المعلومات ، بحث منشور على : http://irbd.hooxs.com/t16012-topic 17/11/2011

(178) أكثر الأساليب انتشارا في فحص المنافذ ويدعى أيضاhalf-open scanning

(179) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

(180) وهي برامج تعطي معلومات مثل النسبة المئوية لزائري الموقع والأوقات التي ينشط فيها الموقع من حيث عدد الزائرين وأوقات الخمول

بروتوكول الزبون للزبون Protocol Client To Client الذي يعطي الصلاحيات للمستخدمين باستقبال أي شيء بدون تقدير للأضرار التي قد تنجم عن ذلك مقارنة بالنظم التي تستخدم برتوكول زبون المزود Client-Server Protocol كما يتم استغلال المنافذ المفتوحة في نظم التشغيل والتطبيقات العاملة معه كالتطبيقات التي تعمل مع التقنيات التي تعتمد على بروتوكول Telnetالتي تسمح بالوصول إلى أجهزة الحاسب الآلي عن بعد وتنفيذ الأوامر إليها(١٨١) . مثلما حصل عندما نجح أربعة تلاميذ يدرسون في إحدى مدارس نيويورك الأمريكية لا تتجاوز أعمارهم الثالثة عشرة من الوصول إلى البيانات التي تقوم شركة أسمنت Lafarge في كندا بتخزينها في بنك معلومات شركة Data pace الأمريكية من خلال اتصالات هاتفية أجريت عن بعد من هاتف المدرسة . وتعد هذه الأخيرة من أكثر الشركات ثقة بين الزبائن لما تتمتع به من إجراءات أمنية تحيط بشبكة المعلومات العائدة لها(١٨٢). وهناك أيضا الألماني Marais Hessالبالغ من العمر ٢٤ عاما الذي نجح من خلال استخدام حاسبه الآلي الشخصي من محل إقامته في هانوفر بألمانيا في التغلغل بطريق الاتصال البعدى لمنظومات ٣٠ حاسب آلي في الولايات المتحدة الأمريكية تحوى معلومات عسكرية وأمنية بالإضافة إلى بعض المعلومات والبيانات المتعلقة بأبحاث علمية. كما يمكن استغلال المنافذ المفتوحة في مزود الويب web server مثل مزود IIS ، كما يمكن النفاذ عبر الشبكة إلى الأجهزة المرتبطة بها ومحاولة العثور على ملفات مشاركة غير محمية ، ويسهل وقت انهيار النظام أو حجب الخدمة عنه أو وقت إعادة إقلاع الطريق أمام المخترق . كما يمكن الاستفادة من تفعيل خيارات المشاركة في الملفات والطباعة File and Sharing Printالموجودة في لوحة التحكم أثناء الاتصال بالإنترنت. واستغلال الخصائص المتوفرة في المتصفح Browser كخاصية الرجوع إلى الخلف ، وتذكر اسم المستخدم وكلمة المرور ، والإكمال الآلي للاسم وفراغات النماذج ، كما يتم استغلال الأخطاء البشرية في البرمجة المقصودة وغير المقصودة.

رابعا: كسر كلمات المرور الخاصة بالشبكات

---

(181) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت
14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376
(182) الدخول غير المشروع على انظمة انظمة المعلومات ، بحث منشور على : http://irbd.hooxs.com/t16012-topic
17/11/2011

قد يتم الدخول غير المشروع عن طريق تجاوز إجراءات الأمن والاستيلاء على كلمات السر العائدة للمستخدمين الشرعيين، تقوم فكرة كسر كلمات السر بصفة عامة على محاولة تخمين هذه الكلمة وتجربتها فان كان التخمين موفقا كان به ، وإلا تتم تجربة كلمة أخرى حتى يتم التوصل إلى الكلمة المناسبة الصالحة للولوج إلى النظام ففي واقعة حدثت في بريطانيا تمكن تلميذ في الخامسة عشرة من عمره من الوصول على معظم الملفات السرية المخزنة بحاسوب إحدى الشركات الكبرى التي تدير نظاما للمشاركة الزمنية في خدمات الحاسب الآلي عن طريق الحصول على كشوف نظام تشغيل البرامج وتحليلها إلى أن توصل إلى اكتشاف الرموز التعريفية الخاصة بالمشتركين المتمثلة في كلمات السر التي تتيح لهم الدخول إلى النظام مما أتاح له ذلك الإطلاع على الملفات السرية المخزنة والقدرة على تعديلها(183).

وهناك عدة أساليب للقيام بذلك من أشهرها أسلوب هجوم القاموس Dictionary Attack والذي يعتمد على كلمات القاموس اللغوي الموجودة في ملف نصي مرفق بالأداة ويتم تجربة هذه الكلمات بطريقة آلية الواحدة تلو الأخرى على أمل أن تكون كلمة السر المستخدمة من بين تلك الكلمات . والأسلوب الثاني هو أسلوب الهجوم الصادر Brute- Force Attack ويقوم على تركيب عشوائي للكلمات عن طريق تجربة الحروف الأبجدية والأرقام بشكل معين وتجربتها فإن لم تنجح يتم تجربة تشكيلة أخرى من الحروف وهكذا حتى الوصول إلى كلمة السر وكسرها. ويتميز هذا الأسلوب الأخير بقدرته على كسر أية كلمة في حين أن الأسلوب الأول لا يمكنه كسر أية كلمة غير تلك الموجودة في القاموس الخاص به(١٨٤).

ومن أشهر البرامج المستخدمة في كسر كلمات المرور Pwdump الذي يعمل مع نظام التشغيل NT4وبرنامج pwdump 2 الذي يعمل مع نظام التشغيل windows2000 وبرنامج Lop trackالذي يستخدم في استخراج كلمات المرور من ملفات الشبكات . أما بالنسبة لبرامج تخمين كلمات المرور(١٨٥) فهي تعمل على جميع الاحتمالات الممكنة لكلمة المرور من حروف وأرقام ورموز، لكنها تستغرق وقتا أطول في التوصل إلى هذه الكلمة إذا احتوت على عدد كبير من الرموز المستخدمة في عمليات التخمين.

---

(183) الدخول غير المشروع على انظمة انظمة المعلومات ، بحث منشور على : http://irbd.hooxs.com/t16012-topic 17/11/2011

(184) حسين الغافري ، الحماية الجنائية لمواقع الإنترنت في ظل قانون المعاملات الإلكترونية العماني٦٩/٢٠٠٨ 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

185 من أكثر هذه البرامج انتشاراً Cracker Jack :، وJohn The Ripper ، Jack The Ripper، وBrute Force Cracker

خامسا: اقتحام نظم تشغيل الشبكات المختلفة:

تقدم بعض المؤسسات برامج تقتحم نظم تشغيل الشبكات المختلفة ، بحيث تسمح بالدخول إلى المزودات العاملة باستخدام صلاحيات مدير الشبكة وبدون معرفة كلمة المرور الخاصة به . وعند تغير كلمة المرور يعمم البرنامج رسالة تنتقل إلى كافة الأجهزة المتصلة بالشبكة يخبرها بتغير كلمة السر الخاصة بمدير الشبكة(١٨٦).

سادسا: الهندسة الاجتماعية:

قد يتم الدخول غير المشروع "الاختراق"عن طرق ما يعرف بالهندسة الاجتماعية Social Engineeringوهو أسلوب من أساليب الاختراق التي تعتمد على العنصر البشري وليس لها أية أبعاد تقنية .حيث يعمد قراصنة الحاسب الآلي إلى استخدام مهاراتهم في الاتصال مع الآخرين ويستعملوا الخداع والكذب ليحصلوا منهم على معلومات ذات طابع تقني يتمكنوا من خلالها من القيام بعملية الاختراق وغالبا ما تتم هذه العملية من خلال المحادثات الهاتفية.

فن يجيده البعض ويستطيع أن يخترق العديد من الشبكات بسهولة كبيرة ، حتى أن واحدا من أشهر القراصنة ويدعى كيفن ميتينك ذكر في كتاب ألفه بعنوان فن الخداع أن أكثر الاختراقات التي قام بها كانت باستخدام هذا الأسلوب(187).

ومن الأساليب المشهورة في هذا المجال أن يتصل الهكر بأحد مدراء الشبكة ويدعّى أنه مستخدما جديدا منتحلا صفة أحد الموظفين الجدد ويطلب معلومات ولوج النظام المخصصة لهذا الموظف الجديد ، أو أن يتصل الهكر بأحد أقسام في المنظمة التي يريد اختراق شبكتها ، ويدعى أنه أحد الفنيين المسؤولين عن الشبكة وأنه كلف بتأكيد اسم المستخدم وكلمة المرور الخاصة بكل موظف في ذلك القسم وبالتالي قد يحصل على اسم مستخدم وكلمة المرور يتمكن بواسطتها من الولوج إلى الشبكة مستغلا الخداع، وعدم معرفة الموظفين بمبادئ أمن المعلومات ، ومن الأمثلة على هذه الطريقة قيام أحد القراصنة بوضع إعلان على لوحة الشركة يعلن فيه أرقاما جديدة للمساعدة ، وقام الموظفون بالاتصال بالرقم وترك معلومات هامة تتعلق بالاسم وكلمة المرور ونوع

---

(186) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

(187)الدخول غير المشروع على انظمة انظمة المعلومات ، بحث منشور على : http://irbd.hooxs.com/t16012-topic 17/11/2011

الصلاحية وغيرها من المعلومات ، حيث أنهم لم يكونوا يعلمون أنهم يتصلون بهاتف قرصان حاسب وبالتالي وقعوا ضحية هذا القرصان.

الفرع الثاني : الاختراق المبطن للشبكات وأنظمة المعلومات

وهذا النوع من الاختراق[١٨٨] لا يتم إلا بوجود عاملين مهمين:

الأول: البرنامج المسيطر ويعرف بالعميلClient والثاني: الخادم Server الذي يقوم بتسهيل عملية الاختراق ذاتها.

وبعبارة أخرى لا بد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج الخادم وفي جهاز المخترق يوجد برنامج العميل.

تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق، ولكنها جميعها تعتمد على فكرة توفر اتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم (Server) الخاص بالمخترق، وجهاز المخترق على الطرف الآخر حيث يوجد برنامج المستفيد أو العميلClient .

وهناك ثلاث طرق شائعة لتنفيذ ذلك [١٨٩]:

أولا: حصان طروادة Trojan Horse

تقوم الفكرة هنا على إرسال ملف باتش صغير يعرف باسم حصان طروادة[١٩٠] لأنه يقوم بمقام الحصان الخشبي الشهير في الأسطورة المعروفة،هذا الملف الصغيرربما يكون أكثر خبثا من الحصان الخشبي بالرواية التي تحمل اسم حصان طرواده ، لأنه حالما يدخل لجهاز الضحية يغير من هيئته ، فلو فرضنا بأن أسمه mark.exe وحذرنا منه الآخرين فأننا سنجده يحمل اسما آخرا بعد يوم أو يومين . لهذا السبب تكمن خطورة أحصنه طروادة ، فهي من جانب تدخل للأجهزة في صمت وهدوء ، ومن جانب آخريصعب اكتشافها خاصة في حالة عدم وجود برنامج جيد مضاد للفيروسات[١٩١] .

---

(188) تطورت طرق الإختراق بأستخدام سكريبتات الجافا وملفات الكوكيزو أثمرت في تجاوز الجدران النارية حيث تحمل ملفات التجسس تلقائيا عبر بارنارات الإعلانات المصاحبة للمواقع او من خلال مرفقات رسائل الماسنجر الخاص بمايكروسوفت حيث لايرصدها هنا الجدرا الناري ويعتبرها من بنود بروتوكولات الإتصال وهذا مايطلق عليه الإختراق المبطن

(189)الدخول غير المشروع على انظمة المعلومات http://irbd.hooxs.com/t16012-topic17/11/2011

د. حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت

http://www.omanlegal.net/vb/showthread.php?t=376 14/11/2011

(190) حسن طاهر داود، مرجع سابق ، صفحه ١٦٩

*حصان طرواده: هي عبارة عن برامج فيروسية لديها القدرة على الاختفاء داخل برامج أخرى أصلية للمستخدم بحيث عندما تعمل البرامج الأصلية ينشط الفيروس وينتشر ليبدأ أعماله التخريبية

(191) جميل عبد الباقي الصغير، المرجع السابق، ص ٢٣

سهير لطفي تقرير حول ندوة الجرائم الاقتصادية المستحدثة عقدت بالقاهرة ٢٠٠١/٤/٢٠، ص ٢٥

وتتم عملية إرسال برمجيات التجسس بعدة طرق من أشهرها البريد الإلكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر فيجد فيه برنامج الباتش المرسل فيظنه برنامجا مفيدا فيفتحه أو أنه يفتحه من باب الفضول ليجده لا يعمل بعد فتحة فيتجاهله ظنا منه بأنه معطوب ويتجاهل الموضوع بينما في ذلك الوقت يكون المخترق قد وضع قدمه الأولى بداخل الجهاز (يقوم بعض الأشخاص بحذف الملف مباشرة عند اكتشافهم بأنه لا يعمل ولكن يكون قد فات الأوان لأن ملف الباتش من الأنواع التي تعمل فورا بعد فتحها وإن تم حذفها) .

وهناك طرق أخرى لزرع أحصنه طروادة غير البريد الإلكتروني كانتقاله عبر المحادثة من خلال برنامج الـــ ICQ وكذلك عن طريق إنزال بعض البرامج من احد المواقع الغير موثوق بها . كذلك يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص. هذا وعند زرع ملف الباتش في جهاز الضحية (الخادم) فأنه يقوم مباشرة بالاتجاه إلى ملف تسجيل النظام Registry . وفي كل مرة يتم فيها تشغيل الجهاز يقوم هذا الملف بثلاثة أمور هي : (١) فتح بوابة أو منفذ ليتم من خلالها الاتصال (٢) تحديث نفسه وجمع المعلومات المحدثة بجهاز الضحية استعدادا لإرسالها للمخترق فيما بعد (٣) وتحديث بيانات المخترق (المستفيد) في الطرف الأخر . إلا أن مهمته الأساسية فور زراعته مباشرة تكمن في فتح منفذ اتصال داخل الجهاز المصاب تمكن برامج المستفيد (برامج الاختراقات) من النفوذ. كما أنه يقوم بعملية التجسس من خلال تسجيل كل ما يحدث بجهاز الضحية ، أو انه يقوم بعمل أشياء أخرى حسب ما يطلبه منه المستفيد كتحريك الفارة أو فتح باب محرك CD وكل ذلك يتم عن بعد. أو عبر بوابات الاتصال(الـــports)[١٩٢] .

ثانيا: عن طريق الـــ IP Address

عند الاتصال بالإنترنت تكون معرّض لكشف الكثير من المعلومات مثل كعنوان جهازك وموقعه ومزود الخدمة الخاص بك وتسجيل كثير من تحركاتك على الشبكة. ولا تتعجب كثيرا حين تعلم

زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي. بحث مقدم للمؤتمر السادس (. للجمعية المصرية للقانون الجنائي. القاهرة، ١٩٩٣

(192) الدخول غير المشروع على انظمة انظمة المعلومات ، بحث منشور على : http://irbd.hooxs.com/t16012-topic 17/11/2011

بأن كثيرا من المواقع التي تزورها تفتح سجلا خاصا بك يتضمن عنوان الموقع الذي جئت منه بتضمن

IP Address ونوع الكمبيوتر والمتصفح الذي استخدمته بل وحتى نوع معالج جهازك وسرعته ومواصفات شاشاتك وتفاصيل كثيرة. فحينما يتمكن مخترق من معرفة رقم الـــ IP الخاص بالضحية فأنه ومن خلاله يتمكن من الولوج إلى الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلا بالشبكة فقط ، ولكن هذا الخيار لا يخدم المخترق كثيرا لأن السير فر الخاص بمزود الخدمة يقوم بتغيير رقم الـــ IP الخاص بالمشترك تلقائيا عند كل عملية دخول للشبكة.

ثالثا: عن طريق الكوكي Cookie

هو عبارة عن ملف صغير تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب ، يحوي بعض الآليات التي تمكّن الموقع الذي يتبع له من جمع وتخزين بعض البيانات عن الجهاز وعدد المرات التي زار المستخدم فيها الموقع ، كما أنها تسرّع عمليات نقل البيانات بين جهاز المستخدم والموقع(١٩٣) ،فالهدف الأساسي منها هو تجاري إلا أنه قد يساء استخدامه من قبل بعض المبرمجين المتمرسين بلغة الجافا Jafa فهذه اللغة لديها قدرات عالية للتعمق أكثر لداخل الأجهزة والحصول على معلومات أكثر عن المستخدم[194].

بعض المواقع على شبكة الانترنت تقوم بإدخال البرامج الصغيرة (MAGIC COKIES) في الملف الخاص بالجهاز بهذا (COCKES FILE) الذي يحتفظ بمعلومات عن المستخدم واختبارات العرض الخاصة به(١٩٥) .

يتضح لنا مما سبق أن الدخول غير المشروع على أنظمة الحاسبات الآلية يتحقق بالوصول إلى المعلومات والبيانات المخزنة داخل النظام دون وجه حق عن طريق استخدام أنشطة غير مشروعة عن طريق خرق حرمة النظام والدخول إليه ، فإن المتطفل يتمكن من الوصول إلى المعطيات الموجودة به وقراءتها ، أو تحميلها ، والوصول لكل ما هو مسموح الوصول إليه

([193])التخلص من الإعلانات والكعكات (Cookies) والمخترقين– دراسة منشورة على شبكة الإنترنت (موقع الحماية والهاكرز) الرابط : http://www.websy.net/learn/hackers/course46.htm ٢٠١١/١١/١٧

([194])حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

([195]) حسن طاهر داود، جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم الأمنية، (١٤٢٠هـ - ٢٠٠٠م) ، ط١، صفحه١٣٤

بالنسبة لصاحب الحساب الأصلي بما في ذلك الوثائق الشخصية والمؤسسية والوثائق الحساسة وقواعد المعلومات .

الفرع الثالث :مدي ضرورة وجود نشاط يسبق الدخول غير المشروع لأنظمة الحاسب الآلي

ثار التساؤل حول ما إذا كان الدخول الذهني المحض دون أن يسبق ذلك أية عملية منطقية يقوم بها الفاعل كافيا لقيام جريمة الدخول غير المشروع أم لا ، بمعنى آخر هل يجب لقيام الجريمة أن يقوم الفاعل بتشغيل الجهاز واستخدام وسائل وطرق معينة بحيث يصل في النهاية إلى النظام ومحتوياته من معلومات وبيانات وبرامج ، بحيث لا يكفي مثلا الإطلاع على هذه المحتويات من على شاشة الجهاز الموجودة عليها لقيام الجريمة طالما أن الفاعل لم يقم بنفسه بإحضارها.

تباينت مواقف التشريعات المختلفة في الإجابة على هذا التساؤل ، حيث ذهبت بعضها إلى ضرورة استخدام وسائل محددة لقيام الجريمة وهو ما يعني القيام بنشاط معين ، كما هو الحال في التشريع العماني في البند الأول من المادة ٢٧٦مكرر الذي اشترط استخدام جهاز الحاسب الآلي في الدخول غير المشروع وذات الشيء في القانون القطري في المادة ٣٧١[١٩٦] الذي استلزمت أن يكون الدخول عن طريق التحايل ، في حين أن البعض الأخر استبعد الدخول الذهني المحض كما هو الحال في القانون الإنجليزي الذي اشترط أن يتم الدخول غير المشروع قد تم عن طريق نشاط ما يتسبب في قيام الحاسب الآلي بأية وظيفة كانت ، مما يعني أنه يجب أن يقوم الحاسب الآلي بوظيفة ما استجابة لنشاط الفاعل. وهذا معناه أن الإطلاع على المعطيات من خلال الشاشة لا يكفي لقيام الجريمة.

وعلى العكس من ذلك نجد تشريعات أخرى لم تتطلب أي نشاط مادي يسبق الدخول إلى النظام ولم تستلزم استخدام وسائل معينة ليتم الدخول بها كما هو الحال في التشريع الفرنسي في المادة ٣٢٣-١ منه[197] والتشريع الأردني في المادة الثالثة/ا من قانون أنظمة المعلومات لعام ٢٠١٠.

ونحن نؤيد الاتجاه التشريعي الأخير ، بان جرّم مجرد الدخول غير المشروع لنظام المعلومات باعتبارها جرائم خطر وذلك لأهمية ما يحويه النظام المعلوماتي من معلومات وبيانات تقدر بالملايين أحيانا.

---

(196) الدخول غير المشروع على انظمة انظمة المعلومات ، بحث منشور على : http://irbd.hooxs.com/t16012-topic 17/11/2011

(197) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

المطلب الثاني: الركن المعنوي لجريمة الدخول غير المشروع لنظام معلومات أو موقع الكتروني

باستقراء نص المادة ٣/أ من قانون أنظمة المعلومات لعام ٢٠١٠ [١٩٨] نستطيع أن نستخلص من عبارة (كل من دخل قصدا..) إن هذه الجريمة تنتمي إلى الجرائم العمدية وبالتالي فإنه يلزم توافر القصد الجنائي والقصد الجنائي يمكن تعريفه بأنه (علم بعناصر الجريمة واراده متجهة إلى تحقيق هذه العناصر)[١٩٩] ، ومن المسلم به في الفقه الحديث إن القانون الجزائي لا يكتفي بقيام الجريمة واستحقاق العقاب عنها بمجرد القيام أو تحقق ركنها المادي بل لا بد إلى جانب ذلك من تحقق ركن معنوي الذي يمثل اتجاها خاطئا يكشف عن الحالة النفسية للجاني عند اقترافه للفعل[٢٠٠] وهذا ما عبرت عنه القاعدة اللاتينية (لا جريمة من غير خطأ وألا مسؤولية في غياب الخطأ)[٢٠١]. ويفترض القصد الجرمي في الجرائم المقصودة علم مرتكب الفعل بتوافر عناصرها وهذا معناه أنه يتعين أن تتجه الإرادة والعلم إلى العناصر المتطلبة بالجريمة كما يحددها القانون ، مما يستلزم أن ينصرف العلم إلى إلى جميع العناصر القانونية للجريمة[٢٠٢].

ويمكن أن يستدل القاضي على توافر القصد الجنائي لدى الجاني إذا كان النظام محاطا بنظام أمني وتم اختراقه من قبل الجاني[٢٠٣].

وعليه يترتب أن يحيط علم الجاني بكل الوقائع التي يترتب على توافرها قيام الجريمة ، فإذا كان جاهلا بالوقائع المادية للجريمة أو وقع غلط في عنصر من عناصرها الواقعية والجوهرية فان ذلك يمنع من توافر القصد الجرمي لديه[٢٠٤].

وطبقا للقواعد العامة فان القصد الجنائي في هذه الجريمة ينتفي إذا كان الجاني قد اعتقد خطأ بأنه له الحق في الدخول أو ما زال له الحق في الدخول إلى النظام الآلي إذا كان قد سبق له الاشتراك

---

(198) المادة٣- أ- كل من دخل قصداً الى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين

(199) نظام توفيق المجالي ،المرجع السابق، صفحة ٣٢٧

(200) محمد حمّاد الهيتي ، مرجع سابق ،صفحة ١٨١

(201) مأمون محمد سلامه ، قانون العقوبات القسم العام، دار غريب للطباعة –القاهره، ١٩٧٦، الطبعة الثانية ، ص٢٢٥،د. صفيه محمد صفوة ، القصد الجنائي والمسؤولية المطلقة ، مطبعة ابن زيدزن –بيروت، ١٩٨٦ الطبعة الاولى ، ص٥٩

(202) نظام توفيق المجالي صفحة، شرح قانون العقوبات القسم العام، دار الثقافة للنشر والتوزيع -عمان، ط١، ص ٣٢٧

(203) محمد أمين الرومي " جرائم الكمبيوتر و الانترنيت " دار المطبوعات الجامعية، طبعة ٢٠٠٣ ، ص ١٠٣

(204) نظام توفيق المجالي ، المرجع السابق، صفحة ٣٢٧

في الدخول إلى البرنامج ولكن مدة الاشتراك كانت قد انتهت استنادا إلى هذا الاعتقاد الخاطئ. لان الغلط في أمر جوهري ينفي القصد.

المطلب الثالث :تجريم مجرد الدخول غير المشروع لنظام معلومات في التشريعات المقارنة

أغلب التشريعات التي تناولت جريمة الدخول غير المشروع لموقع الكتروني تأخذ بتجريم الدخول المجرد إلى النظام المعلوماتى ، حيث أن الجريمة تقوم بمجرد الولوج إلى النظام حتى وإن لم يترتب على فعل الدخول ضررا أو فائدة ، طالما أن ذلك الدخول كان بدون وجه حق . ومن الأمثلة على هذه التشريعات القانون الفرنسي الذي اعتبر أن الدخول المجرد يشكل الركن المادي لجريمة الدخول غير المشروع في صورتها البسيطة (م٣٢٣-١) ، ونفس الاتجاه نجده في التشريع القطري(م٣٧١-٣٧٢) وذات الشيء نجده في قانون الجزاء العماني (البند"١" م٢٧٦ مكرر) حيث نصت على ما يلي: (يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد عن على سنتين وبغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب احد الأفعال التالية :

١. الالتقاط غير المشروع للمعلومات أو البيانات ٢. الدخول غير المشروع على أنظمة الحاسب الآلي ٣. ....) .

وكذلك المادة ٧٦ من مشروع قانون المعاملات والتجارة الإلكترونية العماني، وهو ذاته في التشريع الإماراتي ٢/٢٠٠٦م(البند "١"م ٢)[٢٠٥] حيث نصت على ما يلي : (

١- كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

٢- فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين.[٢٠٦]، وكذلك المشرع الأردني الماد٣/ا من قانون جرائم أنظمة المعلومات لعام ٢٠١٠. والتي نصت على (أ- كل من دخل قصداً إلى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على

([205]) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت
14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

([206]) موقع شبكة المعلومات القانونية لدول مجلس التعاون الخليجي
http://www.gcc-legal.org/mojportalpublic/DisplayLegislations.aspx?LawID=3168&country=2 ٢٠١١/١٠/٢٠

ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين) .[٢٠٧]

الفصل الثاني

جريمة الدخول غير المشروع عن قصد إلى موقع الكتروني أو نظام معلومات بهدف تحقيق نتيجة جرمية

نصت المادة ٣/ب من قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ (ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار أو بكلنا هاتين العقوبتين) باستقراء هذا النص يتبين أن المشرع الأردني قد شدد العقاب بالنسبة إلى جريمة الدخول قصدا إلى موقع الكتروني أو نظام معلومات إذا قصد أو هدف إلى محو أو تعديل أو

---

(207) المادة الثالثة من قانون جرائم أنظمة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

إتلاف في المعطيات المخزنة في الحاسوب الآلي وذلك لان هذه الجريمة أكثر خطورة من الجريمة المنصوص عليها في الفقرة الأولى من القانون ذاته.

ولكي تتحقق أركان هذه الجريمة طبقا للنص الوارد أعلاه يشترط في هذه الجريمة شرطان رئيسيان

أولا: أن يكون الدخول غير المشروع مقصودا بالمعنى القانوني.

ثانيا :أن يهدف من وراء هذا الدخول غير المشروع تحقيق نتيجة جريمة كما وردت في نص المادة ٣ الفقرة /ب وسواء تحققت النتيجة أم لا .

كما أن نصوص المواد (٤ ، ٥ ، ٦ ، ٨ ، ٩ ، ١١) من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ أشارت إلى جريمة الدخول غير المشروع لنظام معلومات أو موقع الكتروني بهدف تحقيق نتيجة جرمية حسب نص كل مادة منهما .

وسوف نتناول هذه الجريمة في ثلاثة مباحث : المبحث الأول الركن المادي لجريمة الدخول غير المشروع لموقع الكتروني بهدف تحقيق نتيجة جرمية والمبحث الثاني الركن المعنوي لها والمبحث الثالث موقف التشريعات المقارنة من هذه الجريمة .

المبحث الأول :الركن المادي لجريمة الدخول غير المشروع لنظام معلومات بهدف تحقيق نتيجة جرمية

يتكون الركن المادي في جرائم الضرر من ثلاثة عناصر هي السلوك الجرمي والنتيجة الضارة التي يعاقب عليها القانون ثم علاقة سببية تربط بين السلوك والنتيجة (٢٠٨).

وقبل البحث في عناصر الركن المادي لجريمة الدخول غير المشروع عن قصد إلى موقع الكتروني أو نظام معلومات بهدف تحقيق نتيجة جرمية لابد من توضيح الطبيعة القانونية لجريمة الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات بهدف تحقيق نتيجة جرمية كمطلب أول وفي المطلب الثاني نتناول السلوك الجرمي (النشاط الجرمي) لهذه الجريمة.

المطلب الأول :الطبيعـــــــــــة القانونية لهذه الجريمـــــــــــة

ما هي الطبيعة القانونية لجريمة الدخول غير المشروع بهدف تحقيق نتيجة جرمية؟

---

(208) نظام توفيق المجالي ،المرجع السابق ، صفحة ٣٢٧

هل تعد من قبيل الجرائم المادية ذات النتيجة أم إنها جرائم شكلية ذات سلوك ونشاط ؟ بمعنى أخر هل يجب أن يكون الدخول غير المشروع منتجا لأثرا ما ، أي يؤدي إلى نتيجة إجرامية محددة كالوصول إلى المعطيات المختلفة التي يحتويها هذا النظام أم إن الجريمة تتم بمجرد الدخول؟ وما محل هذه الجريمة ؟

بداية نشير إلى أن حماية النظام المعلوماتي لا تطرح إشكالا ،بينما حماية المعلومة يثير إشكالات باعتبار أن المعلومة شيء معنوي يثير جدلا فيما يتعلق بقابليته للتملك من عدمها هذا من جهة ومن جهة أخرى هناك من يرى بان في الحماية الجنائية للمعلومة مساس بحرية الإعلام[209].

والمشرع كان موفقا في صياغة هذه المادة القانونية لان هدفه من التجريم هي حماية النظام المعلوماتي في حد ذاته ومنتجاته[٢١٠] بعبارة أخرى هي حماية لهذه المعطيات أو المعلومات[٢١١].

وعليه فان محل الجريمة هو النظام المعلوماتي بما ينتجه من برامج وبيانات ومعطيات .

سبق أن ذكرنا أن الفقه يقسّم الجرائم إلى نوعين جرائم مادية وهي الجرائم ذات نتيجة ، وجرائم شكلية وهي الجرائم ذات سلوك ونشاط بحت . وهذا يثير التساؤل التالي : ما هي طبيعة جريمة الدخول غير المشروع بهدف إلغاء أو تعديل بيانات.. ..حسب المادة ٣/ب من قانون جرائم أنظمة المعلومات لعام ٢٠١٠، هل تعد من قبيل الجرائم المادية ذات النتيجة أم أنها جرائم شكلية ذات سلوك ونشاط فقط؟

برأينا أن هذه الجريمة تعتبر من جرائم الخطر (شكليه)التي لا تتطلب تحقيق نتيجة جرمية بدلالة النص الوارد في المادة ٣/ب (..بهدف إلغاء أو حذف أو إضافة ..بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني..) دون اشتراط تحقيق نتيجة جرميه ، لكن بعد الرجوع إلى المذكرة الإيضاحية لقانون جرائم أنظمة المعلومات[٢١٢] يتبين لنا أنها ساوت بالعقاب على الدخول غير المشروع إذا كان غرض الجاني هو العبث بالمعلومات داخل الكمبيوتر سواء بالتغيير أو بالحذف، أو بالفعل إذا تحققت النتيجة الجرمية بالتغيير أو بالحذف ، ونستنتج من

---

(209)قارة آمال ، الجريمة المعلوماتية رسالة ماجستير ، جامعة الجزائر كلية الحقوق – بن عكنون ٢٠٠٢ صفحه٢٠

(210) مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إداراتها.

(211) عمر الفاروق الحسيني : تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي مجلة المحامي، الكويت، عدد 20.نوفمبر / ديسمبر ١٩٨٩ ، ص٢٠

(212) المذكرة الايضاحية لقانون جرائم أنظمة المعلومات http://www.slideshare.net/UrdunMubdi3/31-72010-2 18/11/2011

*النص الذي ورد في المذكرة الايضاحية :(فإذا كان الدخول بهدف ارتكاب أي من الأفعال أو تحقيق أي من النتائج التي ينص عليها البند (ب) موضوع البحث، فتشدد العقوبة بحق الفاعل على النحو المذكور).

ذلك أن المشرع الأردني ومن باب التحوط لحماية النظام القانوني عاقب إذا كان الدخول غير المشروع بهدف إتلاف أو محو البيانات وذلك بهدف تامين الحماية للنظام المعلوماتي .

لكن نص المادة ٣/ب من قانون أنظمة المعلومات لعام ٢٠١٠يثير تساؤلا وهوماذا لو كان الفاعل مصرحا له بالدخول (أي كان دخوله مشروعا لموقع الكتروني أو نظام معلومات) وقام بحذف بيانات أو إتلافها ، هل تقوم بحقه عقوبة الدخول غير المشروع بهدف إلغاء أو إتلاف بيانات؟

ونحن نرى أن هذا التجريم لا ينطبق ولا يدخل في نطاق تطبيق نص المادة المذكورة أعلاه، وعلة ذلك أن النص القانوني (ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة) أشار إذا كان الدخول غير مشروع لنظام معلومات ولم يتطرق لحالة إذا كان الدخول مشروعا لنظام المعلومات وترتب عليه إتلاف المعلومات ، وبناء على ذلك نرى أنه لا تقوم المسؤولية الجزائية ولا يمكن تطبيق العقوبة الواردة في نص هذه المادة تطبيقا لمبدأ الشرعية الجزائية (لاجريمة ولاعقوبة إلا بنص).

وهنا نجد أن هناك ثغرة في هذا التجريم، إذ كان من الواجب على المشرع الأردني أن يعاقب على التغيير أو الحذف في حد ذاته في مادة قانونية مستقلة ، بالإضافة إلى الدخول غير المشروع بغرض التغيير أو الحذف .

ونقترح في هذا الصدد إضافة مادة قانونية يكون نصها كالتالي: - إذا ترتب على الدخول إلى موقع الكتروني أو نظام معلومات إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها يعاقب بـــ.." .

المطلب الثاني: السلوك الجرمي لجريمة الدخول غير المشروع لنظام معلومات بهدف تحقيق جرمية

تقوم هذه الجريمة على فعل الدخول- المنطقي- غير المشروع ، وذلك بغرض فتح باب يؤدي إلى نظام الحاسب الآلي بمكوناته المنطقية بهدف إتلاف أو محو أو تعديل البيانات... وحيث أن السلوك الجرمي قد يأخذ صورة ايجابية يتطلب من الجاني مباشرة نشاط ايجابي فان النشاط في هذه الجريمة يهدف إلى تحقيق نتيجة جرمية تتمثل في إتلاف أو تعديل ...

والدخول هنا يجب ألا يحمل على المعنى المادي لهذا اللفظ ،وإنما يجب أن يأخذ على انه إجراء اتصال بالنظام بأي طريقة من الطرق اللازمة سواء استخدام الجاني قرصا أو جهاز تلفونيا أو جهاز حاسوبي اخر لديه أو استخدام كارتا ممغنطا أو قام بضرب حروف الرقم السري الذي يحمى به البرنامج على وحدة الإدخال.

والنشاط الجرمي في هذه الجريمة يتم بوسائل عديدة منها استغلال المنافذ المفتوحة بنظم التشغيل أو برامج الحماية ،أو استغلال المنافذ المفتوحة يوجد برنامج الخادم وفي جهاز المخترق يوجد برنامج العميل . بهدف إيقاف الشبكة المعلوماتية أو نظام المعلومات عن العمل،من أمثلة ذلك أن يقوم الفاعل بإرسال إعلانات تجارية spam يغزو بها موقع لشركة ما ، بحيث لا تتمكن من استقبال طلبات الزبائن.

كما يمكن أن يقع النشاط المعاقب عليه بأن يستعمل الجاني فيروسات وهي برامج الغرض منها تدمير أو مسح المعلومات، ونرى بان الجريمة تقع بمجرد زرع الفيروس أو بتحقيق نتيجة مادية معينة مثل التدمير أو المسح للمعلومات أو اضطراب في سير النظام بحيث لا يعمل على الوجه المعتاد الصحيح، كما لو حدث إبطاء في سير النظام أو انفجرت القنبلة المنطقية[٢١٣] بعد وقت معين وأدت إلى إتلاف النظام أو مسح المعلومات.

ومن خلال النصوص القانونية الوارد في قانون جرائم أنظمة المعلومات نلاحظ أن المشرع لم يجرم نتيجة واحدة محددة وإنما جرم التخريب والإتلاف والتعديل والتعطيل للنظام المعلوماتي ، وإلغاء موقع الكتروني وغيرها، فالعبرة ليس بطريقة معينة يتبعها الجاني ، بل بقيامه بسلوك إيجابي يتمثل في استخدام أية وسيلة يحقق بها نتيجة جرمية ،

والواضح أن المشرع يهدف من وراء تغطيته للنتائج السابقة ليس فقط حماية مادة الشيء وإنما بالدرجة الأولى حماية قيمته الاقتصادية بحيث من المتصور وقوع الجريمة رغم بقاء مادة الشيء إذا نجم عن السلوك الإجرامي [٢١٤]انتقاص القيمة الاقتصادية بأن جعله غير صالح للاستعمال أو قلل من قوته في المبادلة التجارية .

وحتى تقوم الجريمة بحق الجاني لا بد من توافر الرابطة السببية بين النشاط الجرمي والنتيجة التي تحققت .

---

[213] القنبلة المنطقية هي احدانواع حصان طرواده وتصمم بحيث تعمل عند حدوث ظروف معينة او لدى تنفيذ امر معين

([214]) جميل عبد الباقي الصغير . المرجع السابق.ص ١٥٣ . وفي نفس هدا المعنى د/ هدى حمد قشقوش : جرائم الكمبيوتر والجرائم(الأخرى في مجال تكنولوجيا المعلومات . بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي الذي انعقد في القاهرة في 28 اكتوبر ١٩٩٣ .ص ٥٦٤

وسوف نتناول النشاط الجرمي الذي يؤدي إلى النتيجة الجريمة (الإتلاف أو التعديل أو المحو أو الحذف...) في إطار واسع من خلال تناول النتيجة الجرمية والنشاط الجرمي :

الفرع الأول: إتلاف نظام المعالجة الآلية

في هذا المطلب سوف نوضح معنى الإتلاف ومن ثم بيان الوسائل الفنية التي يتحقق بها الإتلاف على النحو التالي:

أولا:معنى الإتلاف

وسوف نناقش في هذه الدراسة الإتلاف في المجال المعلوماتى . وذلك في محورين اثنين: الأول يتعلق بالماهية القانونية لهذا النوع من الإتلاف ، والثاني يتعلق بالموقف التشريعي منه

ويقصد بالإتلاف هو تخريب الشيء محل الجريمة بإتلافه أو التقليل من قيمته وذلك بجعله غير صالح للاستعمال أو تعطيله[٢١٥]، وبمعنى أخر تعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية. فهو إفناء لمادة الشيء أو على الأقل إحداث تغيرات شاملة عليها ، بحيث يكون غير صالح إطلاقا للاستعمال في الغرض المخصص له.

والإتلاف في المجال المعلوماتى قد يقع على المكونات المادية المتصلة بالحاسب الآلي وملحقاته كالشاشة أو لوحة المفاتيح أو الفارة أو الأشرطة أو الأقراص الممغنطة وغيرها[٢١٦] مما له علاقة بهذا المجال . وهنا يسمى إتلافا ماديا ولا توجد أية عقبات قانونية تحول دون تطبيق النصوص التقليدية الخاصة بجريمة الإتلاف المادي على اعتبار أن محل الجريمة مال مادي منقول مملوك للغير ، وفعل الإتلاف بهذا المعنى يخضع للنصوص التقليدية في قانون العقوبات التي تتناول تجريم فعل الإتلاف الذي يؤدي بإلحاق الضرر بالمال المنقول المملوك للغير وذلك سندا لنص المادة(٤٤٥)من قانون العقوبات الأردني التي تنص على مايلي:" كل من الحق باختياره ضررا بمال الغير المنقول يعاقب على بناء الشكوى المتضرر بالحبس بمدة لا تتجاوز السنة أو بغرامة لا تتعدى خمسين ألف دينار أو بكلتا العقوبتين". وتثور في بعض الأحيان مسالة إتلاف أوراق الحاسب الالكتروني وشبكاته مما يؤثر على برامجه وبياناته أو على سير عمل النظام المعلوماتي[٢١٧].

ونحن نرى أن إتلاف أوراق الحاسب تدخل في نطاق التجريم الواردة في النصوص التقليدية (قانون العقوبات الأردني) ،أما بالنسبة لإتلاف المادة التي تقع على منشات الاتصالات التي تشمل

([215]) محمود محمود مصطفى، المرجع السابق، ص٦٤٦ ،د. محمود نجيب حسني ، جرائم الاعتداء على الاموال في قانون العقوبات اللبناني ، دراسه مقارنه ١٩٨٤ص٤٩٦

([216]) نهلا المومني ، المرجع السابق، ص١٢٤

([217]) سامي حمدان الرواشده/د.أحمد موسى الهياجنه، مكافحة الجريمة المعلوماتية بالتجريم والعقاب : القانون الانجليزي نموذجا، بحث محكم منشور في المجلة الاردنية في القانون والعلوم السياسية ، المجلد(١) العدد(٣) تشرين الاول ٢٠٠٩ ص١٣٧

بالضرورة شبكة الانترنت ومنشاتها المادية فقد عالجها المشرع الأردني- بشكل خاص – وذلك في قانون الاتصالات رقم(١٣) لسنة ١٩٩٥ إذ نصت المادة (٧٢) من هذا القانون على مايلي:

ا-كل من أقدم قصدا على تخريب منشات الاتصالات أو الحق بها ضررا عن قصد يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين أو بغرامه لا تقل عن (٢٠٠) دينار ولا تزيد عن (٥٠٠٠) دينار أو كلتا العقوبتين وتضاعف العقوبة إذا تسبب فعله بالتعطيل حركة الاتصالات.

ب-كل من تسبب إهمالا في تخريب منشات الاتصالات أو الحق الضرر بها يعاقب بالحبس لمدة لاتزيد عن ثلاثة اشهراو بغرامة لا تزيد عن (١٠٠) دينار أو بكلتا العقوبتين.

وبذلك كفل المشرع حماية منشات الاتصالات ومنها منشات شبكة الانترنت المادية من الاعتداء بإتلافها أو إلحاق الضرر بها وبالإضافة إلى الحماية التي كفلها للأموال المعنوية من الإتلاف في المواد(٧٦،٧٧،٨٠) من ذات القانون[٢١٨].

ويرى البعض[٢١٩] أن الإتلاف الواقع على المكونات المادية للحاسب الآلي يخرج عن إطار الجريمة المعلوماتية على اعتبار أن هذه الأخيرة تتصل بالأفعال التي تشكل اعتداء على المعلومات المبرمجة ونظم معالجتها باستخدام طرق ووسائل خاصة ، وبالتالي لا حاجة إلى إفراد نصوص خاصة لإتلاف المكونات المادية للحاسب الآلي، حيث أنه بالإمكان تطبيق النصوص التقليدية عليها[٢٢٠]. ومع ذلك تناولت بعض التشريعات إتلاف المكونات المادية للحاسب الآلي في نصوص خاصة ترتبط بالجريمة المعلوماتية منها على سبيل المثال المادة ٥٠٢ من قانون العقوبات الخاص بولاية كاليفورنيا الأمريكية التي تجرّم إتلاف وتخريب أنظمة المعالجة الآلية للمعلومات بمكوناتها المادية والمعنوية[٢٢١]، وأيضا المادة ٣٧٤ من قانون العقوبات القطري ٢٠٠٤/١١ التي نصت على معاقبة كل من يتلف أو يخرب عمدا وحدات الإدخال أو الإخراج أو

---

(218) سامي حمدان الرواشده/د.أحمد موسى الهياجنه، مكافحة الجريمة المعلوماتية بالتجريم والعقاب ، مرجع سابق ص١٣٧ ،محمد امين الشوابكه، جرائم الحاسوب والانترنت، الطبعة الاولى، دار الثقافة، عمان، ٢٠٠٤ ،ص٢١٩

(219) حسين بن سعيد الغافري ، الجرائم الافتراضية وجهود سلطنة عمان التشريعية في مواجهتها ورقة عمل قدمت في المؤتمر العلمي الأول " الجوانب القانونية للمعلوماتية بين النظرية والتطبيق " كلية الحقوق – جامعة السلطان قابوس في الفترة من ١٣ – ٢٠١١/٣/١٤ م

Waslk (Martin) : crime and computer ,Oxford University ,press 1991, p136 ; Vergucht (Pascal): op. cit, p .123

(220) سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت ""دراسة مقارنة"" ، دار النهضة العربية-القاهره، ٢٠٠٩ ،ط١،ص ٥٢

(221) Conley (Jonhn M) & Bryan (Robert M) : A survey of computer crime legislation in United States , I.C.T.L , Vol .8.1, 1999, P41.

شاشة الحاسب الآلي مملوك للغير أو الآلات أو الأدوات المكونة له . بالحبس مدة لا تجاوز ثلاث سنوات وبالغرامة التي لا تزيد عن العشرة آلاف ريال قطري[٢٢٢].

فالإتلاف الوارد في الجرائم الالكترونية هو الإتلاف الواقع على المكونات أو الكيانات المنطقية – المعنوية – للحاسب الآلي والتي يقصد بها كل العناصر غير المادية التي يتكون منها نظام الحاسب الآلي كالمعلومات والبيانات والبرامج على اختلاف أنواعها ووظائفها . وهنا يتبادر التساؤل حول مدى صلاحية هذه المكونات كمحل لجريمة الإتلاف بالصورة الكلاسيكية المعروفة عندما لا يترتب على المساس بها إتلاف أي من العناصر المادية التي يتكون منها نظام المعالجة الآلية للحاسب الآلي؟

وللخروج من دائرة الخلاف والنقاش وللنأي عن اللجوء إلى القياس الذي يتعارض مع مبدأ الشرعية الجزائية ، أوجد المشرّع الأردني حلا تشريعيا لذلك ، حيث جرّم الدخول غير المشروع بهدف إتلاف المكونات المنطقية لأنظمة الحاسب الآلي بنص الفقرة (ب) من المادة ٣ من قانون جرائم أنظمة المعلومات ويتضح لنا من خلال النص السابق أن النتيجة الجرمية تتحق بالإتلاف ويعني بها إفناء هذه المعلومات وإهلاكها كليا أو جزئيا .

وهذه النتيجة الجرمية تتحقق بنشاط جرمي يتمثل بعدة طرق ووسائل فنية وتقنية مستخدمة لإتلاف هذه المكونات ، و سوف نتناول هذه الوسائل تحت عنوان (الطرق الفنية لإتلاف المكونات المنطقية للحاسب الآلي).

ثانيا :الطرق الفنية لإتلاف المكونات المنطقية للحاسب الآلي

تتنوع الطرق الفنية والتقنية المستخدمة في إتلاف المعلومات والبيانات والبرامج والتي تشكل في مجملها المكونات المنطقية للحاسب الآلي. إلا أن أخطرها على الإطلاق استخدام الشفرة الخبيثة Malicious Software وهي برمجيات ضارة[٢٢٣] وتعد من أخطر العناصر التي تهدد أمن المعلومات والبيانات لأنها تؤدي إلى فقد النظام أو فقد تكامله أو تؤثر على كفاءة أدائه [٢٢٤] ، كما تؤدى إلى إتلاف البرامج وضياع المعلومات، وهي مصممة لتنتقل من حاسب آلي إلى آخر ومن

---

(222) حسين بن سعيد الغافري،ورقة بحثيه بعنوان الجوانب القانونية للمعلوماتية بين النظرية والتطبيق، مقدمة في المؤتمر العلمي الاول ا في جامعة السلطان قابوس في الفترة في الفترة من ١٣ – ٢٠١١/٣/١٤ م

(223) البرامج الضارة تتضمن الفيروسات وبرامج التجسس التي تستخدم لسرقة المعلومات الشخصية أو إرسال الرسائل التطفلية أو ارتكاب الجرائم الاحتيالية

(224) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

شبكة إلى أخرى بهدف إجراء تعديلات في أنظمة الحاسوب عمدا وبدون موافقة مالكي أو مشغلي هذه الأنظمة حتى وقت قريب كان تصنيف هذه البرامج ينقسم إلى ثلاث فروع فقط وهي :

الفيروسات

ديدان الإنترنت

أحصنة طروادة

ولكن مع تطور هذه البرامج والتكنولوجيا المستخدمة فيها تم تحديث طريقة التصنيف لبرامج الهاكرز (البرامج الضارة) إلى برامج سريعة التكاثر والانتشار, برامج للتجسس وإرسال المعلومات و برامج التحكم عن بعد و الهجوم المنسق و برامج جديدة من أحصنة طروادة تجمع من كل بحر قطرة([٢٢٥]).

ولمزيد من التفصيل عن هذه البرمجيات الضارة ، ارتأينا أن نقسم البرمجيات الضارة حسب التقسيم القديم إلى عدة فئات على النحو التالي:

أولا : الفيروساتVIRUS[226]

من المؤكد أن أكثر جرائم الحاسب الآلي إمعانا في الشر هي جريمة النشر الفيروسي ، و الفيروسات عبارة عن برمجيات مشفرة للحاسب الآلي مثل أي برمجيات أخرى يتم تصميمها بهدف محدد وهو إحداث أكبر ضرر ممكن بأنظمة الحاسب الآلي([٢٢٧]) ، وتتميز بقدرتها على ربط نفسها بالبرامج الأخرى وإعادة إنشاء نفسها حتى تبدوا وكأنها تتكاثر وتتوالد ذاتيا ، بالإضافة إلى قدرتها على الانتشار من نظام إلى أخر ، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات بحيث يمكنها أن تنتقل عبر الحدود من أي مكان إلى أخر في العالم.

وعادة ما تسمي باسم أول مكان تكتشف فيه أو باسم مصممها. والفيروس يتميز بثلاث خواص هي التضاعف ، التخفي ، إلحاق الأذى بالآخرين. ويتمثل النشاط التدميرى لها في أنها تقوم بمسح البيانات والمعلومات المخزنة على وسائط التخزين وإتلافها لذا يطلق على هذه العملية اسم مسح البيانات وتحويلها إلى صفر. ZEROING

([225]) تصنيف برامج الهاكرز، بحث منشور على الانترنت : http://www.oocities.org/tona55555/index-4.htm ٢٠١١/١١/٢٦

([226]) هو جزء من برنامج ذو أهداف شريرة يتم إلحاقه ببرنامج الحاسب الآلي ، وعند التنفيذ البرنامج الملوث يبدأ انتشار الفيروس ، انظر حسن طاهر داود، المرجع السابق ، صفحه ١٦٩

([227]) هدى حامد قشقوش، المرجع السابق ،ص١١٦

ومن أبرز الهجمات الفيروسية التي شهدها عالم الحاسبات والمعلومات هجوم الفيروس الباكستاني المعروف باسم المخ Brain واقتحامه لحوالي ٣٥٠ألف من حاسبات IBM والحاسبات المتوافقة معه[٢٢٨].

وللفيروسات أنواع متعددة فهي تنقسم من حيث التكوين والأهداف إلى : فيروسات عامة العدوى تصيب أي برنامج أو ملف موجود في جهاز الحاسب الآلي ، وهناك فيروسات محدودة العدوى حيث تصيب نوع معين من النظم وتتميز عن سابقتها بأنها بطيئة الانتشار ، وهناك فيروسات عامة الهدف تمتاز بسهولة الإعداد واتساع القوة التدميرية لها وغالبية الفيروسات تندرج تحت هذا النوع ومن الأمثلة عليها فيروس مايكل انجلوا الذي ظهر في ١٩٩٢/٣/٢٦م. وهناك فيروسات محدودة الهدف تقوم بتغير الهدف الأصلي من عمل البرنامج أو الملف التي تصيبه دون أن تصيبه بالعطل.وهو يحتاج إلى مهارة عالية ومعرفة بالتطبيق المستهدف ومن الأمثلة عليه فيروس ماك ماج Mac Mag الذي ظهر عام ١٩٨٨ م[٢٢٩].

أما من حيث الأضرار التي تحدثها بأنظمة الحاسب الآلي فبعضها تصيب الملفات التنفيذية و يقصد بالملفات التنفيذية تلك الملفات التي تكون من نوع EXE ، COM، BAT، حيث أن تلك الملفات هي المسئولة عن تشغيل البرامج الموجودة على الحاسب وبالتالي فإن إصابة هذه الملفات يؤدي إلى تعطيل البرنامج بالكامل –خاصة النوع الأول والثاني، أما النوع الثالث فيكاد يكون غير مستخدم في نظم التشغيل الحالية.

والبعض الآخر من الفيروسات يؤدي إلي عدم قدرة نظام التشغيل على التعامل مع الملفات بالرغم من أن هذه الملفات مازالت موجودة علي القرص الصلب ولم يتم حذفها ومن أشهر هذه الفيروسات فيروس تشرنوبل[230].

وهناك من الفيروسات الشائعة ينصب تأثيرها على برامج معالجة النصوص حيث تقوم بإدخال كلمات وعبارات وجمل غير مرغوب فيها وغير متوقعة ، وهو غالبا ما يقوم بتعديل الأمر "حفظ" ليشغل نفسه بعد ذلك تلقائيا ، وقد تصيب أيضا الملفات الخاص بمستندات النصوص النشطة

([228]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([229]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([230]) وهو من أخطر الفيروسات لأنه قادر على مسح القرص الصلب و اصابة البرنامج الأساسي المسؤول عن المخرجات و المدخلات للجهاز مما قد يتسبب في تلف اللوحة الأم

HTMLالمحتوية على نصوص جافا وأنواع أخرى من الرموز التنفيذية ، مما يؤدي إلى انتشارها، ومن الأمثلة على هذه الفيروسات فيروس ميليسا(٢٣١) الذي ظهر ١٩٩٩ والذي انتشر عبر البريد الإلكتروني.out lock .

ومنذ عام ٢٠٠٤حدث تطور كبير في طريقة تصميم الفيروسات خاصة فيروسات الإنترنت التي غالبا ما تعتمد على شبكة الإنترنت حيث أصبحت لا تحتاج إلى الرسائل الإلكترونية لكي تصل إلى ضحاياها من الحاسبات الشخصية والخادمة كفيروس خطوط الإنترنت بلا ستر وبلسيا اللذان ظهرا في أواخر عام ٢٠٠٣ وانتشرا على خطوط الإنترنت حول العام ، فهما وبمجرد أن تشعر بأن أحد الحاسبات قد اتصل بالإنترنت تقوم على الفور بالانتقال له وإصابته(٢٣٢) .

ثانيا برامج الدودة : Worm Software

هي عبارة عن برامج تقوم باستغلال أية فجوة في أنظمة التشغيل لكي تنتقل من حاسب لآخر ، أو من شبكة لأخرى عبر الوصلات التي ترتبط بها وذلك دون حاجة إلى تدخل إنساني لتنشيطها (٢٣٣) وهذا هو الاختلاف بينها وبين حصان طروادة الذي دائما ما يعتمد على التدخل الإنساني لمباشرة نشاطه كما سنرى لاحقا ، كذلك هي لا تلتصق بأنظمة التشغيل في أجهزة الحاسب الآلي التي تصيبها مثلما تفعل الفيروسات كما رأينا . وتتكاثر هذه البرامج أثناء عملية انتقالها بإنتاج نسخ منها ودونما الحاجة إلى برامج وسيطة تساعدها على التكاثر، وتعمل على تقليل كفاءة الشبكة أو التخريب الفعلي للملفات والبرامج ونظم التشغيل.

ولقد ظهرت هذه النوعية من البرامج الضارة لأول مرة في عام ١٩٨٨ على يد الطالب الأمريكي Roper Tappan Morrisوهي ما عرفت بدودة موريس(٢٣٤) Morris ، التي تسببت في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة ، بالإضافة إلى إعاقة طريق مسلك الشبكات ، ناهيك عن الخسائر المادية الكبيرة في مواجهة هذه الدودة.

([231]) و هي من أسرع الفيروسات التي أنتشرت في عام ١٩٩٩ و هي من نوع ماكرو فيروس متخصص في اصابة البريد الإلكتروني وهي تقوم بالإنتشار عن طريق الإلتصاق في برامج النصوص كملحق في رسالة البريد الإلكتروني وما أن يقوم المستخدم بفتح الملف الملحق بالرسالة الا و يبدأ الفيروس بالعمل حيث يستطيع الوصول الى قائمة المراسلة الخاصة بالمستخدم ليقوم بإرسال نفس الرسالة الى أول خمسين عنوان دون علمك و تستمر على نفس المنوال

([232]) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، بحث منشور على http://www.omanlegal.net/vb/showthread.php?t=376 14/11/2011

[233] حسن طاهر داود، المرجع السابق ، صفحه ١٦٩

([234]) الفيروسات إرهاباً تهدد أنظمة المعلومات ، مقال مقدم من الدكتور أمجد حسا ن إلى مؤتمر " الإرهاب في عصر الرقمي" "الذي عقد في جامعة الحسين بن طلال معان -الاردن"١٢/٧/٢٠٠٨-١٠

ومن أشهر أشكال برامج الدودة عبر الإنترنت والتي ظهرت حديثا تلك المعروفة باسم دودة الحب " Love Bug"(٢٣٥)والتي ظهرت إلى الوجود في الرابع من مايو ٢٠٠٠م وتسببت في خسائر تقدر بملاين الدولارات في العديد من المؤسسات مثل NASA وإدارة الأمن القومي الأمريكية SACوالعديد من الشركات والمؤسسات التجارية.

ثالثا: حصان طروادة Trojan Horse

هي عبارة عن برامج فيروسية لديها القدرة على الاختفاء داخل برامج أخرى أصلية للمستخدم بحيث عندما تعمل البرامج الأصلية ينشط الفيروس وينتشر ليبدأ أعماله التخريبية ، وهو يختلف عن الفيروس في أنه لا يتكاثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته يحمل في طياته توقيت وأسلوب استيقاظه ، وهو يؤدي إلى تعديل هذه البرامج وتزوير المعلومات ومحو بعضها . وقد يصل الأمر إلى تدمير النظام بأكمله.

وهذه البرامج هي في الأساس من الناحية التقنية برمجيات اختراق وتجسس تهدف إلى جمع المعلومات والبيانات كاسم المستخدم وكلمات السر الخاصة به وغيرها ومن ثم إرسالها إلى صاحب البرنامج أو مصممه ، وغالبا ما يتم ذلك والمستخدم الضحية متصل بشبكة الإنترنت ، حيث توجد بعض المواقع التي تحمل حصان طروادة في ملفات خاصة تسمي الكوكيز (236)
COOKIES FILEالتي تلحق مستخدم الشبكة أثناء تصفح الشبكة ، فيلحق الأذى بالجهاز وبخصوصية المستخدم. ولا توجد نوعية واحدة لحصان طروادة إذ يندرج تحته العديد من الأنواع من بينها برامج قامت بكتابتها بعض شركات البرمجيات الكبرى ، وعندما يقوم أحد المستفيدين باستخدام أحد منتجات هذه الشركات تقوم هذه البرامج بعمل حصر شامل لكل مكونات النظام المادية والمنطقية الخاص بالمستفيد وعند اتصال المستفيد بشبكة الإنترنت يتم إرسال هذه المعلومات إلى تلك الشركات التي تستخدمها في عملياتها التسويقية ومن أبرز هذه الشركات شركة مايكروسوفت . وهناك قصة نشرتها إحدى الصحف العربية عن أجهزة اتصال متطورة للغاية حصلت عليها إحدى الدول العربية من دولة عظمى على سبيل الهدية تبين بعد فحصها أنها تحتوى

---

(235) و هو مشابه لفيروس مليسا و لكنه متخصص في إصابة برنامج مايكروسوفت أوت لوك لإدارة البريد الإلكتروني و لقد أثار الرعب في بداية هذا العام نتيجة لسرعة انتشاره

(236) لمزيد من الاطلاع انظر التخلص من الإعلانات والكعكات (Cookies) والمخترقين– مرجع سابق http://www.websy.net/learn/hackers/course46.htm ٢٠١١/١١/١٧

على حصان طروادة أعد خصيصا لجمع معلومات عن استخدام الجهاز وعن التردد التي استخدمت عليه(٢٣٧).

رابعا: القنبلة المعلوماتية Bomb

هي نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخرى . فشكليا هي ليست ملفا كاملا متكاملا وإنما شفرة تنضم إلى مجموعة ملفات البرامج وذلك بتقسيمها إلى أجزاء متفرقة هنا وهناك حتى لا يمكن التعرف عليها بحيث تتجمع فيما بينها بحسب الأمر المعطى لها في زمن معين أو حدوث واقعة معينة ، فهي مصممة بحيث تبقي ساكنة وغير فعالة إلا في الزمن المحدد أو الواقعة المحددة (٢٣٨) لذا يتعذر اكتشافها لمدة قد تصل لأشهر وأعوام ، ويؤدي اجتماعها هذا إلى انعدام القدرة على تشغيل البرنامج عبر جهاز الحاسب الآلي. وتستخدم هذه البرامج لإتلاف المعلومات والبيانات وتغيير برامج ومعلومات النظام.وقد تستخدم كبرامج لحماية الملكية الفكرية من القرصنة وخاصة تلك التي تحدث عبر شبكة الإنترنت ، فالذي يملك حقوق النسخ قد يجيز للغير نسخ مصنفه عبر شبكة الإنترنت إلا أن هذه الإجازة قد تكون لفترة محددة بفترة زمنية قصيرة تختفي بعدها البرمجية أو الملف المنسوخ بسبب القنبلة الموقوتة

وتعرف القنبلة المعلوماتية بمصطلح الشفرة الموقوتة Disabling Code وأكثر ما تبرز في البرامج المؤقتة التي تشتمل عليها الحملات الإعلانية كما هو الشأن في المجلات التي يوزع معها بعض الأسطوانات الهدية والتي تحتوى على بعض البرامج ، وهناك أيضا بعض المواقع على شبكة الإنترنت التي تشتمل على بعضا من هذه البرامج ، وهذا النوع من البرامج الضارة ينقسم إلى قسمين هما:

١. القنبلة المنطقية Logic Bomb : وهذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدأ التشغيل أو عند إنجاز أمر معين في الحاسب الآلي أو عند بدأ تشغيل برنامج معين.

ومن الأمثلة على ذلك زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف بحيث تنفجر لتمحو سجلات الموظفين الموجودة أصلا في المنشأة مثلما حصل في ولاية لوس أنجلس الأمريكية عندما

([237]) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، بحث منشور على http://www.omanlegal.net/vb/showthread.php?t=376 14/11/2011

([238]) وليد عاكم ، التحقيق في جرائم الحاسوب ، بحث منشور على الانترنت http://www.wasmia.com/jazy/crime09.pdf ٢٠١١/١٠/١٥

تمكن أحد الأشخاص العاملين في إدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها ، مما أدى إلى تخريب النظام عدة مرات[٢٣٩].

2.القنبلة الزمنية[٢٤٠] :Time Bomb وهنا البرنامج ينشط في تاريخ معين محدد بالذات فهو يثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم.

ومن الأمثلة الواقعية قيام شخص يعمل بوظيفة محاسب خبير في نظم المعلومات بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة بدافع الانتقام ، حيث انفجرت بعد مضي ستة أشهر من رحيله عن المنشأة وترتب على ذلك إتلاف كل البيانات المتعلقة به[٢٤١].

خامسا:الباب الخفي Back Door

نشأت هذه البرامج في الأصل كآلية يستخدمها المبرمجون لتضمن لهم مدخلا خاصا للأنظمة التي يقومون ببرمجتها ، خاصة عندما يتسبب خطأ برمجي في التوقف التام للنظام [٢٤٢]، وفي بعض الأحيان يقومون بذلك لأسباب خبيثة أو على الأقل مشبوهة. ومع الوقت أصبحت تستخدم من قبل الهكر في الولوج الأنظمة المعلوماتية ، وإختراقها.

وأنوع شفرة الباب الخفي كثيرة ومتعددة ، ولكنها تجتمع في كونها تعطي ولوجا خاصا يتجاوز الإجراءات الروتينية ، ورغم أن البعض يخلط بينها وبين حصان طروادة إلا أنه يمكن التفريق بينهما من حيث أن الأخير يوحي للمستخدم بأنه برنامج ذو منفعة ، في حين أن برامج الباب الخفي تقوم بعملها في الخفاء.

سادسا : برمجيات ويب التفاعلية

قد يسيء بعض المبرمجين توظيف بعض البرمجيات المخصصة لمواقع الإنترنت التفاعلية والتي تكون عبارة عن ملفات تنفيذية يتم تحميلها وتشغيلها على جهاز المستخدم فور اتصاله بالموقع الموجودة عليه ، ومن هذه البرمجيات برمجيات جافا وأكتف أكس[٢٤٣] ، ورغم أن هاتين الوسيلتين صممتا بهدف تسهيل تفاعل زوار مواقع الإنترنت إلا أنه متى ما تم برمجتها عن قصد

([239]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([240]) وليد عاكم ، التحقيق في جرائم الحاسوب ، بحث منشور على الانترنت http://www.wasmia.com/jazy/crime09.pdf ٢٠١١/١٠/١٥

([241]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([242]) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، بحث منشور على http://www.omanlegal.net/vb/showthread.php?t=376 14/11/2011

([243]) حسن طاهر داود، المرجع السابق ، ص١٦٩

بأعمال أخرى يمكنها أن تلحق بأجهزتهم الكثير من الأضرار. و يتفق الفقهاء في انجلترا و الولايات المتحدة على المشكلات القانونية التي تنشأ عن جميع الفيروسات تكون غالبا واحدة ، فلا وجه للتفرقة بين الفيروس و الدودة وحصان طروادة لأنها ترتب نفس الآثار[244].

الفرع الثاني:إضافة البيانات أو المعلومات Introduction .

يقصد به إضافة معطيات جديدة لم تكن موجودة من قبل على الدعامة الخاصة سواء كانت خالية أو كان يوجد بها معطيات [٢٤٥]، وذلك قد يتم بهدف التشويش على صحة البيانات والمعلومات القائمة ، والسؤال هنا هل يترتب على هذا الإدخال إتلافا لأي من مكونات الحاسب الآلي المنطقية؟

لو نظرنا إلى التشريعات المختلفة التي جرّمت الإتلاف المعلوماتى لوجدنا أن الكثير منها اعتبرت الإدخال غير المشروع للمعلومات صورة من صور الركن المادي لهذه الجريمة كما هو الحال في المادة ٣٢٣-٣ من قانون العقوبات الفرنسي الجديد والمادة ١٧ من قانون إساءة استخدام الحاسبات الآلية في المملكة المتحدة ، والمادة ٣٧٣ من قانون العقوبات القطري ١١/٢٠٠٤ ، والمادة٨٣ من مشروع المعاملات والتجارة الإلكترونية العماني،والمادة ٦ من قانون مكافحة جرائم تقنية المعلومات الإماراتي ٢/٢٠٠٦م ، والفقرة الأولي من المادة الرابعة من الاتفاقية الأوربية للإجرام المعلوماتى[٢٤٦] ،والمادة ٣ /ب والمادة ٤ من قانون جرائم أنظمة المعلومات الأردني لعام ٢٠١٠ [٢٤٧].

بالإضاالثالث:لك ذهب القضاء الفرنسي في تطبيق جريمة إتلاف المكونات المنطقية لأنظمة الحاسب الآلي إلى اعتبار هذه الصورة مكونا لهذه الجريمة ، حيث أدانت محكمة استئناف باريس عام ١٩٩٠ أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسب الآلي ، كما ذهبت محكمة جنح ليموج عام ١٩٩٤م إلى إدانة المتهم بتهمة إتلاف المكونات المنطقية للحاسب الآلي لقيامه بإدخال برنامج خبيث " حصان طروادة" إلى نظام الحاسب الآلي مما ترتب عليه إتلافا للمعلومات فضلا عن إعاقة النظام عن أداء وظائفه ، كما ذهبت محكمة النقض الفرنسية في حكم لها عام ١٩٩٦م إلى أن إدخال البرامج الخبيثة إلى نظام الحاسب

---

[244] جرائم الانترنت ، بحث منشور على الانترنت : http://www.djelfa.info/vb/showthread.php?t=492535 ٢٠١١/١٠/١٦

([245]) فشار عطاء الله ، مواجهة الجريمة المعلوماتية في التشريع الجزائري ،بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية تم عقده بأكاديمية الدراسات العليا بليبيا فى أكتوبر ٢٠٠٩ صفحة ١٧

([246]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([247]) قانــون جرائــم أنظمــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

الآلي هو سلوك معاقب عليه تطبيقا للفقرة الثانية من المادة ٣٢٣ من قانون العقوبات ، كما ذهبت نفس المحكمة أيضا في حكم لها صادر عام ١٩٩٩ إلى أن إدخال بيانات يترتب عليها إتلاف لأي من المكونات المنطقية لنظام الحاسب الآلي هو سلوك معاقب عليه ولو كان للجاني حق الدخول إلى هذا النظام[248].

الفرع الثالث :تدمير البيانات والمعلومات :Destruction

تعد هذه الصورة هي الأخطر والأبعد أثرا عن باقي صور الإتلاف. فقد أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ١٩٩٤م بتجريم الأفعال التي تؤدي إلى تدمير المعلومات [٢٤٩]، وتشمل هذه الأفعال : المحو ويقصد به إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام ، أو تحطيم تلك الدعامة ، أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة ،والإتلاف ويقصد إفناء مادة الشيء أو هلاكه كليا أو جزيئا ، والتعطيل ويقصد به توقف الشيء عن القيام بوظيفته فترة مؤقتة ، والتخريب ويعني توقف الشيء تماما عن أن يؤدي منفعته كليا أو جزيئا. في حين نجد أن التوصية الصادرة من المجلس الأوروبي بشأن الجرائم المعلوماتية قد ميزت بين شكلين من أشكال التدمير الذي يلحق بالمعلومات ، الأول يتعلق بمحو المعلومات تماما ، والثاني بإخفاء المعلومات بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محوها تماما[250].

وفي دارسة قامت بها وزارة الداخلية الكويتية ذهبت إلى أن الصور المستخدمة في تدمير المعلومات والبيانات والتي تعد من جرائم الحاسب الآلي تشمل الشطب والإلغاء والمسح والإتلاف .ولقد نصت الكثير من النصوص العقابية التي جرمت الإتلاف الواقع على المكونات المنطقية للحاسب الآلي على هذه الصورة باعتبارها إحدى صور الركن المادي لهذه الجريمة منها على سبيل المثال المادة ٣٢٣-٣ من قانون العقوبات الفرنسي الجديد ، والمادة ٢٧٦مكرر "١" من قانون الجزاء العماني ، والمادة ٣٧٢ من القانون القطري ٢٠٠٤/١١ ، والمواد ٢/٢ و ٦ من القانون الإماراتي ٢٠٠٦/٢م ، والمادة٨٣ من مشروع المعاملات والتجارة الإلكترونية

---

(248) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥
http://forum.kooora.com/f.aspx?t=16193884

(249) فشار عطاء الله ، مواجهة الجريمة المعلوماتية في التشريع الجزائري ،بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية تم عقده بأكاديمية الدراسات العليا بليبيا فى أكتوبر ٢٠٠٩

(250) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥
http://forum.kooora.com/f.aspx?t=16193884

العماني[251] ، والمادة ٣ /ب والمادة ٤ من قانون جرائم أنظمة المعلومات الأردني لعام ٢٠١٠. [٢٥٢]

الفرع الرابع :التعديل غير المشروع عن قصد للمعلومات والبيانات :Modification

هذه الصور تعد من أكثر صور الإتلاف شيوعا وانتشارا ، ويقصد بها إجراء نوع من التغير غير المشروع للمعلومات والبيانات المحفوظة داخل النظام واستبدالها بمعطيات ومعلومات جديدة باستخدام إحدى وظائف الحاسب الآلي[253] .

ولقد فرقت التوصية الصادرة عن المجلس الأوروبي بين التعديلات غير المشروعة التي تؤدي إلى نتائج سلبية وبين التعديلات أيضا غير المشروعة والتي تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي ونظامه ، حيث طالبت التوصية بإدراج التعديلات ذات الآثار السلبية ضمن القائمة الأساسية للجرائم المعلوماتية ، في حين أنها اكتفت بخصوص التعديلات ذات النتائج الإيجابية بإدراجها ضمن القائمة الاختيارية .إلا أن الدول التي جرّمت الإتلاف المعلوماتى لم تعتد بهذه التفرقة ، حيث نجدها تجرم كافة أشكال التعديلات وإن اختلفت فيما بينها في تحديد هذا التعديل ومن هذه التشريعات المادة ٣٢٣-٣ من قانون العقوبات الفرنسي الجديد ، والمادة ١٧ من قانون إساءة استخدام الحاسبات الآلية البريطاني ١٩٩٠م والبند السادس من المادة ٢٧٦مكرر من قانون الجزاء العماني ، والمادة ٣٧٣ من قانون العقوبات القطري ٢٠٠٤/١١م والمواد ٢/٢و٦ من القانون الإماراتي ٢٠٠٦/٢م ، والمادة٨٣ من مشروع المعاملات والتجارة الإلكترونية العماني والمادة ٢٦ من المشروع الفلسطيني.[٢٥٤] ، والمادة ٣ /ب والمادة ٤ من قانون جرائم أنظمة المعلومات الأردني لعام ٢٠١٠ . ([٢٥٥])

([251]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([252]) قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

([253]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([254]) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

([255]) قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

المبحث الثاني :الركن المعنوي لجريمة الدخول غير المشروع لنظام معلومات بهدف تحقيق نتيجة جرمية

ليست الجريمة كيان مادي وإنما هي كذلك كيان نفسي ايضا ، وإذا كان الركن المادي يتكون من السلوك المحظور في جرائم الخطر أو السلوك المحظور والنتيجة الجرمية والعلاقة السببية بينهما في جرائم الضرر ، فان الركن المعنوي الذي يتمثل في الوصول الإرادي لماديات الجريمة والسيطرة عليها ، هو وجهها الباطني والنفساني ، فلا محل لمساءلة شخص عن جريمة ما لم تقم صلة أو علاقة بين ماديات الجريمة وإرادته .

فإذا ثبت بان إنسان لم يرد تلك الماديات ، لم يرد ما صدر عنه من أفعال واثار ، امتنعت نسبة تلك الماديات لهذا الإنسان ،وترتب على ذلك تخلف كل من الركن المادي والمعنوي على حد سواء.

وعليه إذا لم تتجه إرادته إلى إحداثها ، أطلق على موقفه هذا (الخطأ) ، والخطأ ينفي المسؤولية الجانية العمدية لانتفاء القصد الجنائي التي لا تقوم بدونه[٢٥٦].

والسؤال ما الحكم إذا لم يبين النص القانوني صورة الركن المعنوي ؟ للإجابة على هذا السؤال نقول أن ما توافقت عليه التشريعات الجزائية كافة ، هو اعتبار المسؤولية على أساس القصد هي الأصل والمسؤولية على أساس الخطأ استثناء على الأصل ، وينبغي تبعا لذلك أن تستند المسؤولية في إقرارها إلى صراحة نص القانون بحيث إذا لم يبين المشرع صورة الركن المعنوي اعتبر هذا ارتدادا للأصل وتطلبا للقصد الجرمي[٢٥٧] ، ونلاحظ أن النص الوارد في المادة الثالثة من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ أشار بالنص أن تكون إرادة الجاني مقصودة لارتكاب جريمة الدخول غير المشروع لنظام المعلومات، ولذلك كان من الضروري أن نتاول الركن المعنوي وبيان مفهوم القصد الجرمي بنوعيه القصد العام والقصد الخاص لهذه الجريمة كمطلب أول ، وان نتناول الخطأ كمطلب ثاني.

---

(256) كامل السعيد، المرجع السابق ، صفحة ٢٧٧

(257) كامل السعيد ، المرجع السابق ، صفحة ٢٧٩

المطلب الأول :القصد العام والقصد الخاص لجريمة الدخول غير المشروع لنظام المعلومات بهدف تحقيق نتيجة جرمية

الركن المعنوي هو الركن الثاني من أركان الجريمة وسوف نتناول في هذا المطلب القصد العام كفرع أول والقصد الخاص كفرع ثاني

الفرع الأول : القصد العام

تنتمي هذه الجريمة إلى الجرائم العمدية وبالتالي فإنه يلزم توافر القصد الجنائي من علم وإرادة وبالتالي لو حدث الدخول بطريق الخطأ فإن الجريمة لا تقوم.

المادة ٦٣ من قانون العقوبات العقوبات الأردني عرفت القصد العام على انه (إرادة ارتكاب الجريمة على ما عرفها القانون)[٢٥٨].

والقصد الجنائي يكتمل بناؤه بتوافر عنصري العلم والارداة ، وعليه يمكن تعريف القصد الجرمي بأنه (علم بعناصر الجريمة وإرادة متجهة إلى تحقيق هذه العناصر)[٢٥٩].

ويفترض القصد الجرمي في الجرائم المقصودة علم مرتكب الفعل المكون للجريمة بتوافر عناصرها وهذا معناه أنه يتعين أن تتجه الإرادة والعلم إلى العناصر المتطلبة بالجريمة كما يحددها القانون ، فما تتجه إليه الإرادة يتعين أن يحيط به العلم أولا مما يستلزم أن ينصرف العلم إلى جميع عناصر القانونية للجريمة [٢٦٠].

ونطاق العلم كأحد عناصر القصد الجرمي يشمل العلم بالوقائع والقانون معا وعليه يترتب أن يحيط علم الجاني بكل الوقائع التي يترتب على توافرها قيام الجريمة ، فإذا كان جاهلا بالوقائع المادية للجريمة أو وقع غلط في عنصر من عناصرها الواقعية والجوهرية فان ذلك يمنع من توافر القصد الجرمي لديه[٢٦١].

الفرع الثاني : القصد الخاص

وهنا لابد من التطرق إلى بيان التفرقة بين الدافع (الباعث) والقصد الجرمي ، فالدافع (الباعث) ، الغرض ، الغاية ، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة ، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا،حيث اعتبر البعض

---

[258] قانون العقوبات الاردني لعام ١٩٦٠ المنشور في الجريدة الرسمية بتاريخ ١٩٦٠/١/١

[259] نظام توفيق المجالي، المرجع السابق، صفحة ٣٢٧

[260] نظام توفيق المجالي ، المرجع السابق، صفحة ٣٢٧

[261] نظام توفيق المجالي ، المرجع السابق ، صفحة ٣٢٧

الباعث "لا اثر له في وجود القصد الجنائي"(٢٦٢)، لكن المشرع الأردني أشار في المادة ٦٧ /٢ من قانون العقوبات الأردني بأن الدافع لا يكون عنصرا في التجريم إلا في الأحوال التي نص عليها القانون "(٢٦٣) ، بمعنى أن القاعدة القانونية هي التي تقرر أن الدافع عنصر في التجريم وليست القاعدة القضائية وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب ، فانها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية. فالباعث (الدافع) هو "العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام"(٢٦٤) وهو اذن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو "يختلف من جريمة إلى أخرى، تبعا لاختلاف النـــــــــــاس من حيث السن والجنس ودرجة التعليم وغير ذلك مـــــــــن المؤثرات كما يختلـــــــــف بالنسبـــــــــة للجريمة الواحدة من شخــــــــــص لآخر"(265)..

أما الغرض، "فهو الهدف الفوري المباشر للسلوك الإجرامي ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات" (٢٦٦) وأما الغاية، "فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام أو سلب مال المجني عليه في جريمة القتل"(267).

والأصل أن الباعث والغاية ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين ، علم الجاني بعناصر الجريمة ، واتجاه إرادته إلى تحقيق هذه العناصر أوالى قبولها. ولا تأثير للباعث أوالغاية "على قيام الجريمة أو العقاب عليها، فالجريمة تقوم بتحقق عناصرها سواء كان الباعث نبيلا أو رذيلا وسواء كانت الغاية شريفة أو دنيئة. وإذا كانت القاعدة أن الباعث أو الغاية لا أثر لهما على قيام الجريمة، فان القانون يسبغ عليهما في بعض الأحيان أهمية قانونية خاصة" (٢٦٨) وبالنسبة لجرائم الكمبيوتر والانترنت ، فثمة دوافع عديدة تحرك الجناة لارتكاب جريمة الدخول غير المشروع وهي تقريبا نفس الدوافع التي تدفع الجناة لارتكاب باقي الجرائم الالكترونية ، ونلاحظ أن المشرع الأردني في قانون جرائم أنظمة المعلومات شدد العقاب في

---

(262) أحمد فتحي سرور، الوسيط في قانون العقوبات ـ القسم العام، الطبعة الخامسة دار النهضة العربية، القاهرة، ١٩٩١. ص ٤٢٧.
(263) المادة (٦٧) من قانون العقوبات الاردني رقم ١٦ صدر في الجريدة الرسمية عدد (١٤٨٧) بتاريخ ١٩٦٠-٠١-٠١
(264) كامل السعيد ، المرجع السابق، صفحه٢٩١
(265) فوزية عبد الستار، شرح قانون العقوبات ـ القسم العام، بدون ذكر رقم الطبعة، دار النهضة العربية، القاهرة، ١٩٩٢. ص ٤٧٩.
(266) كامل السعيد ، المرجع السابق ،ص ٢٩١
(267) كامل السعيد ، المرجع السابق ، صفحه ٢٩٢
(268) حسني ، المرجع السابق ، ص ٤٨٠.

حالة إذا كان الدخول غير المشروع بهدف (الغاية) تحقيق نتيجة جرمية في المواد (٦، ٧، ٨، ٩) ويمكننا من خلال الحالات التطبيقية التالية تبيان الدوافع الرئيسة مع الإشارة لنصوص قانون جرائم انظمة المعلومات لعام ٢٠١٠التي أشارت إلى تلك :

أولا: السعي إلى تحقيق الكسب المالي

يعد هذا الدافع والذي يمثل في الحقيقة غاية الفاعل)من بين أكثر الدوافع تحريكا للجناة لاقتراف جرائم الحاسوب ، ذلك أن خصائص هذه الجرائم ، وحجم الربح الكبير الممكن تحقيقه من بعضها، خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع[٢٦٩].

ففي دراسة قديمة عرض لها الفقيه Parker يظهر أن ٤٣% من حالات الغش المرتبط بالحاسوب المعلن عنها قد بوشرت من أجل اختلاس المال، وهي النسبة الأعلى من بين النسب التي حققتها جرائم أخرى في هذه الدراسة (٣٢% سرقة معلومات ١٩% أفعال إتلاف ١٥% سرقة وقت الحاسوب (الآلة) لأغراض شخصية) [270].

وقد أشار المشرع الأردني إلى هذا الهدف (القصد الخاص) فشدد العقاب إذا كان الدخول غير المشروع بهدف تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية ، حيث نصت المادة السادسة من قانون جرائم أنظمة المعلومات لعام ٢٠١٠على ما يلي:(المادة٦- أ- كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٢٠٠٠) ألفي دينار أو بكلتا هاتين العقوبتين.

ب- كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصداً دون سبب مشروع بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية للحصول لنفسه أو لغيــــــره على بيانـــات أو

---

(269) يونس عرب ، " صور الجرائم الالكترونية " ورقة عمل قدمت في ندوة " تطوير التشريعات في مجال مكافحة الجرائم الالكترونية " التي نظمتها هيئة تنظيم الاتصالات / مسقط – سلطنة عمان ٢-٤ ابريل ٢٠٠٦

(270) سامي الشوا، الغش المعلوماتي كظاهرة اجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ٢٥-٢٨ تشرين أول / أكتوبر ١٩٩٣

معلومات أو أموال أو خدمات تخص الاخرين يعاقب بالحبس مدة لا تقــــــل عن سنـــــة وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار) [٢٧١].

وإذا ما انتقلنا للدراسات الحديثة ، فسنجد أن هذا الدافع يسود على غيره ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية .

ثانيا : الانتقام من رب العمل وإلحاق الضرر به

لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل ، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح كما أسلفنا، لكنها في حالات كثيرة ، مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من المنشأة أو رب العمل ، وتحديدا جرائم إتلاف البيانات، والبرامج وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيس والتكنيك الغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.

ثالثا: الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية

يرى البعض [٢٧٢] "أن الدافع إلى ارتكاب الجرائم الحاسوبية من قبل الجاني، يغلب عليه الرغبة في قهر النظام أكثـــــــــــر من شهوة الحصول على الربح" ومع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها، إذ يظهر السعي إلى تحقيق الربح دافعا أكثر تحريكا لجرائم الحاسوب من الرغبة في قهر النظام إلا أن الدافع الأخيـــــر، يتجســـــــــد في نسبـــــــــة معتبـــــرة من جرائم الحاسوب خاصة ما يعرف بأنشطة الـــ - (hackers) المتطفلين الدخيلين على النظام والمتجسدة في جرائم التوصل مع أنظمة الحاسب – تحديدا عن بعد – والاستخدام غير المصرح به لنظام الحاسوب ، واختراق مواقع الانترنت. ويميل مرتكبو هذه الجرائم "إلى إظهار تفوقهم ومستوى ارتقاء براعتهم.

---

(271) قانـــون جرائــــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

(272) سامي الشوا، الغش المعلوماتي كظاهرة اجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ٢٥-٢٨ تشرين أول / أكتوبر ١٩٩٣ ، انظر كذلك د. جميل عبد الباقي ، المرجع السابق ، ص ١٦

رابعا:دوافع أخرى

هناك من الجرائم الافتراضية يكون الهدف (القصد الخاص) أو الدافع من وراء ارتكابها دوافع سياسية تتمثل في تهديد الأمن القومي والعسكري وظهور ما يعرف بحرب المعلومات و التجسس الإلكتروني والإرهاب الإلكتروني، وكانت تقارير صحافية ذكرت في منتصف ٢٠٠٩ قيام جهات صينية غير معروفة باختراقات كبيرة على شبكة الإنترنت طالت مئات الحواسيب في زهاء ١٠٣ بلدان، وذكر المركز الكندي أن شبكة تجسس الكترونية تعمل من الصين تمكنت من اختراق ١٢٩٥ جهاز حاسب آلي في ١٠٣ بلد[٢٧٣]. وقد شدد المشرع الأردني العقاب إذا كان الدخول غير المشروع بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني أو إتلافها ، حيث نصت المادة الحادية عشر من قانون جرائم أنظمة المعلومات لعام ٢٠١٠على ما يلي : (١١-أ- كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع الكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٥٠٠٠) خمسة ألاف دينار.

ب- إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة ، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها ، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (١٠٠٠) ألف دينار ولا تزيد على (٥٠٠٠) خمسة آلاف دينار) . [٢٧٤]

ونلاحظ أن المشرع في الفقرة (ب) من هذه المادة قد تدرج بالتشديد في العقاب بحيث اعتبر الدخول غير المشروع بهدف إتلاف إلغاء البيانات التي تمس الأمن القومي جناية يعاقب عليها بالأشغال الشاقة وذلك لفداحة الجرم المرتكب .

وهناك من الجرائم الافتراضية يكون الهدف (القصد الخاص) أو الدافع من وراء ارتكابها الترويج للدعارة أو الأعمال الإباحية ، وقد شدد المشرع الأردني العقاب إذا تم استخدام الشبكة

---

(273) تحقيق بعنوان (دول العالم تنتقد الصين على التجسس المعلوماتي) ، منشور في جريدة النهار اللبنانية بتاريخ ٠٥ / ٠٧ / ٢٠٠٩ http://ucipliban.org/arabic/index.php?option=com_content&task=view&id=12285&Itemid=313 ٢٠١١/١١/١٢

(274) المادة (١١) من قانون جرائم أنظمة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

المعلوماتية أو أي نظام معلومات للترويج للدعارة أو الأعمال الإباحية في نصوص المواد (٨، ٩) من قانون جرائم أنظمة المعلومات لعام ٢٠١٠[٢٧٥]

وهناك من الجرائم الافتراضية يكون الهدف (القصد الخاص) أو الدافع من وراء ارتكابها القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم إرهابي وقد شدد المشرع الأردني العقاب إذا تم استخدام الشبكة المعلوماتية أو أي نظام معلومات لدعم أو القيام بأعمال إرهابية ، حيث نصت المادة العاشرة من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ على ما يلي : (المادة ١٠ – كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو انشأ موقعاً الكترونياً لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة.[٢٧٦]

ومن المسلم به أن القانون في الجرائم المقصودة يكتفي بالقصد العام لكنه في جريمة الدخول غير المشروع بهدف إتلاف أو القيام بأعمال تجسسية أو إرهابية أو ترويج للدعارة ..الخ ،لم يكتف المشرع الأردني بتطلب القصد الجنائي العام من علم وإرادة، بل استلزم توافر القصد الجنائي الخاص الذي يتمثل في ضرورة توافر نية من نوع خاص وهو قصد الجاني من الدخول غير المشروع أن يكون بغرض إتلاف أو محو أو تعديل أو حذف البيانات بالنظام أو بالبيانات التي يحتويها أو بهدف نشر الدعارة أو التجسس أو الإرهاب أو يكون غرضه تغيير تصميم موقع إلكتروني أو إتلافه أو تعديله أو شغل عنوانه.

---

[275] المواد (٨،٩) من قانون جرائم أنظمة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

[276] المادة (١٠) قانون جرائم أنظمة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

المطلب الثاني :الخطأ في جريمة الدخول غير المشروع لنظام معلومات

لم يرسم قانون العقوبات الأردني نظرية عامة للخطأ ولم يعاقب على كل نتيجة تبني على خطأ، ومادام أن المشرع لم يعتبر الخطأ سببا عاما للمسؤولية الجزائية في كل الأحوال ، بل اقتصر بالنص على أحوال معينة ، فانه لا يجوز القياس عليها أو التوسع فيها[٢٧٧] .

وطبقا للقواعد العامة فان القصد الجنائي في هذه الجريمة ينتفي أو لايتحقق إذا كان الجاني قد اعتقد خطأ بأنه ما زال له الحق في الدخول إلى النظام الآلي كان يكون قد سبق له الاشتراك في الدخول إلى البرنامج ولكن مدة الاشتراك كانت قد انتهت وذلك دخل إلى النظام استنادا إلى هذا الاعتقاد الخاطئ.

لان الغلط في أمر جوهري ينفي القصد[٢٧٨].

والسؤال الذي يطرح نفسه في هذا المقام :ماذا لو وجد نفسه الجاني قد دخل النظام عن طريق الخطأ ولم يقم بقطع الاتصال هل يتحقق القصد الجرمي الذي تقوم به جريمة الدخول غير المشروع ؟ نجيب هذا التساؤل بان الدخول بطريقة الخطأ إلى البرنامج ينفي القصد الذي تقوم به هذه الجريمة ، أي بعبارة أخرى أن المستخدم إذا بدا متجردا من القصد كما لو وجد الشخص نفسه قد دخل إلى النظام أو إلى جزء غير مسموح له بالدخول إليه عن طريق الخطأ ، لكن ماذا لو وجد في هذا الاتصال استحسانا ومتعة فظل يتابع تجواله ولم يتولى قطع الاتصال الذي ليس له الحق في إجراءه ، فإننا في هذه الحالة لا بد من استنباط قرينة القصد الجرمي من خلال طول الفترة الزمنية التي قضاها متجولا في النظام الحاسوبي ، فإذا كانت الفترة طويلة نسبيا يمكن اعتبار دخوله إلى النظام غير مشروع بصورة الدخول دون تصريح أو بما يجاوز التصريح ويعود تقديرها للمحكمة صاحبة الاختصاص ، بينما نلاحظ أن المشرع الفرنسي قد انتبه إلى النتائج التي تترتب على مثل هذه الحالة اذ من السهل على الجاني أن يدعي أن الاتصال قد تم عن طريق الخطأ لذلك فقد جرم المشرع الدخول إلى البرنامج عن طريق الخطأ ومن ثم البقاء به وعدها جريمة مستقلة هي جريمة الإبقاء على الاتصال أو المكوث فيه ، فالمادة ٣٢٣-١ من قانون العقوبات الفرنسي تجرم صراحة الدخول أو البقاء غير المصرح يهما داخل كل أو جزء من نظام المعالجة الآلية للمعلومات (.....أو مكث في داخل النظام المعالجة الآلية للمعطيات أو في جزء منه) وتطبيقا لهذا ذهبت محكمة استئناف باريس في حكم لها صادر بتاريخ ١٩٩٩/٤/٥م

---

(277) كامل السعيد ، المرجع السابق ، صفحه ٣١٣

(278) محمد حماد الهيتي ، المرجع السابق ، ص١٨٩

إلى أن القانون يجرم البقاء غير المشروع داخل نظام الحاسب الآلي سواء أكان الدخول قد تم بطريق الخطأ أو تم بطريقة مشروعة إلا أنه اكتسب بعد ذلك صفة عدم المشروعية كما لو فقد الفاعل صفة البقاء نتيجة لخطاء من جانبه(٢٧٩).

المبحث الثالث :موقف التشريعات المقارنة من جريمة الدخول غير المشروع بهدف تحقيق نتيجة جرمية

نظرا لما للمكونات المنطقية لأنظمة الحاسب الآلي والمواقع الالكترونية وما تشمله من برامج ومعلومات وبيانات من قيمة اقتصادية ، سارعت الدول إلى فرض حمايتها لتلك المكونات و جرّمت كل ما من شأنه الإضرار بها خاصة إذا تم عبر شبكة الإنترنت وفي المطلب الثاني سوف نخصصه لموقف التشريعات المقارنة من جريمة الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات بهدف تحقيق نتيجة جرمية .

في حين أن البعض الأخر من التشريعات يشترط تحقق نتيجة معينة كما هو الحال في التشريع الفيدرالي الأمريكي لجرائم الحاسب الآلي(م ١١٠٣٠– (a) - ، (2– (a) -1030اللتان تعاقبان على الدخول غير المصرح به متى ما أعقبه الحصول على بعض المعلومات. والبند الثاني من المادة ٥٢ من قانون المعاملات الإلكترونية العماني ٢٠٠٨/٦٩م الذي جرم الدخول غير المشروع متى ما ترتب عليه تعطيل الأنظمة أو إتلاف البرامج الحاسوبية أو سرقة المعلومات (٢٨٠) . .

وعلى بالرغم من ذلك فالموقف التشريعي لم يكن واحداً في جميع الدول. لذا فإن دراستنا لهذه الجزئية سوف تكون من خلال محورين اثنين مقسمة إلى:الأول يبحث موقف التشريعات في بعض الدول الغربية ، في حين أن الثاني يبحث موقف التشريعات في بعض الدول العربية.

المطلب الأول :موقف بعض التشريعات الغربية

أولى المشرّع الغربي المكونات المنطقية لأنظمة الحاسب الآلي وما تشمله من برامج ومعلومات وبيانات اهتماما خاصة نظرا لما لها من قيمة اقتصادية كبيرة خاصة في عصر عرف بكونه

---

(279) قارة آمال ، الجريمة المعلوماتية رسالة ماجستير ، جامعة الجزائر كلية الحقوق – بن عكنون ٢٠٠٢ ، صفحه٤٤

(280) حسين الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، بحث منشور 14/11/2011http://www.omanlegal.net/vb/showthread.php?t=376

عصر المعلوماتية ، وتمثل هذا الاهتمام الغربي في استحداث نصوص خاصة تجرّم كل ما من شأنه الإضرار بتلك المكونات[281].

الفرع الأول: الوضع في التشريع الفرنسي

تعتبر فرنسا من أوائل الدول الغربية التي سارعت إلى إصدار تشريعات خاصة بحماية النظم المعلوماتية والتصدي لبعض صور الجرائم المستحدثة ، والتي قد تقع بسبب التقدم في استخدام الحاسب الآلي وكذلك شبكة الإنترنت أو بعض الشبكات المحلية كما هو الحال في شبكة المانتيل الفرنسية[282].

ويعد القانون رقم ١٧-٧٨ الصادر في السادس من يناير١٩٧٨م بشأن الحريات والمعلومات هو اللبنة الأساسية لتنظيم وحماية النظم المعلوماتية في فرنسا حيث عالج المشرّع من خلاله مسألة تخزين البيانات في الحاسب الآلي وبيان لأنواعها المختلفة ومدة التخزين ، كذلك الجهة المختصة بالرقابة والإشراف على أعمال ذلك القانون.

بعد ذلك وعلى أثر التطور الكبير في ثورة المعلومات وفي الحاسبات الآلية وشبكة الإنترنت تقدم النائب Jacques Godjrain في الخامس من أغسطس باقتراح مشروع قانون خاص بالغش المعلوماتى والذي تم إقراره في ١٩٨٧/١٢/٢٢م ليصبح قانونا نافذا اعتبارا من الخامس من يناير١٩٨٨م وحمل رقم ١٩-٨٨ بشأن الغش المعلوماتى. وفي وقت لاحق أدمجت نصوص هذا القانون في قانون العقوبات الفرنسي الجديد (المواد ٣٢٣-١ إلى ٣٢٣-٧) تحت عنوان " الاعتداءات على نظام المعالجة الآلية للمعطيات."

ومن أهم ما جاء به هذا القانون فيما يتعلق بالإتلاف المعلوماتى نص المادة ٣٢٣-١ والخاصة بجريمة الدخول غير المشروع على أنظمة الحاسب الآلي، حيث اعتبر الإتلاف الواقع على المعطيات الموجودة داخل النظام ظرفا مشددا لجريمة الدخول غير المشروع متى ما كان الإتلاف بسبب هذه الجريمة الأخيرة. وهناك أيضا المادة ٣٢٣-٣ التي جرّمت إدخال البيانات بطريقة غير

---

(281) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

(282) جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت ٢٠١١/١١/١٥ http://forum.kooora.com/f.aspx?t=16193884

مشروعة في نظام معالجة البيانات أو إلغاء أو تعديل البيانات التي يحتوى عليها النظام بطريقة غير مشروعة.

ومع أن المشرع الفرنسي قد استخدم عبارات متعددة للإشارة إلى الإتلاف ، حيث بين أن الإتلاف يمكن أن يحصل عن طريق التعطيل أو الإفساد أو المحو أو تعديل فان الذي يبدو لنا آن تعطيل أو إفساد برامج حاسب الآلي لا يمكن أن يتم إلا من خلال إدخال المعطيات أو المعلومات أو بيانات جديد أو محو أو تعديل المعطيات أو برامج المختزنة بالجهاز، لان هذه الأفعال من شانها تعطيل تشغيل النظام بصورة كلية أو جزئية وهذا يتحقق من خلال إدخال فيروسات التي سبق أن بينا أن أثره لا ينصرف فقط على برامج التشغيل بل من ممكن أن يمتد أثرها إلى الأنظمة الأخرى .

الفرع الثاني: الوضع في الاتفاقية الأوربية

تتكون اتفاقية بودابست الموقعة ٢٠٠١/١١/٢٣ م من ديباجة وثماني وأربعون مادة موزعة على أربعة فصول : الأول يعالج استخدام المصطلحات ، والثاني يعين الإجراءات الواجب اتخاذها على المستوى الوطني ، الثالث مخصص للتعاون الدولي ، والفصل الرابع يحدد الأحكام الختامية [٢٨٣].

جرّمت هذه اتفاقية والمتعلقة بالإجرام المعلوماتي[٢٨٤] الإتلاف التي تتعرض له المكونات المنطقية للحاسب الآلي ونصت على عدة صور يتم بها الإتلاف المعلوماتي كالإلغاء والإفساد والتدمير وغيرها ، حيث نصت في الفقرة الأولى من المادة ٤ على " تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية وغيرها من الإجراءات الأخرى كلما كان ذلك ضروريا لإصدار نصا قانونيا أو تشريعيا بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها ، عند ارتكابها عن قصد ، وذلك من حيث إتلاف ، أو إلغاء ، أو إفساد ، أو تغيير ، أو تدمير البيانات الموجودة بالكمبيوتر دون وجه حق.

والهدف من وراء تقرير هذا النص وكما أشارت المذكرة التفسيرية لهذه الاتفاقية ضمان حماية مماثلة للبيانات والبرامج المعلوماتية كتلك التي تتمتع بها الممتلكات المادية ضد الخسائر والأضرار التي تحدث لها عن عمد.

---

(283) هلالي عبد الاله احمد ، الجوانب الموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعه في ٢٠٠١/١١/٢٣ ، دار النهضة العربية ، مصر ، طبعة ٢٠٠٣ ، ص١

(284) صالح أحمد البربري دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٠٠١/١١/٢٣ www.arablawinfo.com الدليل الإلكتروني للقانون

الفرع الثالث: الوضع في التشريع البريطاني

جرّم المشرع الانجليزي الدخول غير المصرح به للنظام المعلومات بموجب المادة الأولى من قانون إساءة استخدام الحاسوب لعام ١٩٩٠[٢٨٥]

وتجرم المادة الأولى عدد كبيرا من التصرفات والأفعال مثل : (١)نسخ البرامج وتوزيعها داخل الشبكة باستخدامها من قبل موظفين آخرين خلافا الاتفاقية الرخصة الخاصة بالبرنامج (٢) استخدام النسخ المقلدة من البرنامج بدون موافقة صاحب الرخصة (٣)السماح باستخدام البرنامج المرخص باستخدامه من قبل شركات أو أشخاص آخرين غير مرخص لهم باستخدامه خلافا لاتفاقية الرخصة دون آن ينطوي ذلك على نسخ البرنامج (٤)استخدام البرنامج لغاية أخرى غير الغاية المتفق عليها في اتفاقية الرخصة .[٢٨٦]

وفي عام ٢٠٠٦صدر قانون الشرطة والعدالة (the police and justice act 2006) وقد تم بموجبه تعديل نص المادة الأولى من قانون إساءة استخدام الحاسوب وذلك بموجب المادة (٣٥) من قانون الشرطة والعدالة لعام ٢٠٠٦ وجاء هذا التعديل استجابة إلى قرار الاتحاد الأوروبي فيما يتعلق بانتهاك أنظمة المعلومات الذي اعتمده من قبل مجلس وزراء الاتحاد الأوروبي الصادر ٢٠٠٥/٥/٢٤ ويهدف هذا القرار إلى تحقيق التقارب بين الدول الجزائية للدول الأوروبية من حيث الجرائم والعقوبات والاختصاص وعليه فان تعديل قانون إساءة استخدام الحاسوب جاء لتحقيق الانسجام مع القرار الصادر عن الاتحاد الأوروبي الذي ألزم كافة دول الاتحاد الأوروبي ضرورة العمل على تنفيذ مضمون القرار عن طريق تعديل التشريعات الوطنية ذات العلاقة قبل ٢٠٠٧/٢/٢٤ وذلك من اجل التأكد من وجود عقوبات كافية وفاعلة للمعاقبة على هذا النوع الخطير من السلوك الاجرامي .

أهم التعديلات التي أجريت على المادة الأولى هي[٢٨٧]:

١. إن المسؤولية الجزائية تنهض في موا جهة الفاعل إذا تمكن من الدخول إلى النظام المعلوماتي بنفسه أو إذا مكّن شخص اخر من الدخول إليه إن هذا التعديل جاء منسجما مع الاجتهاد القضائي من جهة كما انه وسع من نطاق التجريم على نحو يمكن القول بان القانون أصبح أكثر فاعلية في التعامل مع هذا النوع المستحدث من الإجرام.

---

(285) سامي حمدان الرواشده/د.أحمد موسى الهياجنه، مكافحة الجريمة المعلوماتية بالتجريم والعقاب ، مرجع سابق ص١٣٧
See also:Peter AIldrige، "Computer Misuse Act 1990"International Banking Law1990،(9)6 ،339-342

(286) سامي حمدان الرواشده/د.أحمد موسى الهياجنه، المرجع السابق ص١٢٩

(287) سامي حمدان الرواشده/د.أحمد موسى الهياجنه، المرجع السابق ص١٣١

٢. شدد المشرع العقوبة لتصبح الحبس لمدة لا تزيد عن سنتين بعد أن كان العقوبة لا تتجاوز ٦ أشهر.

٣. ترتب على زيادة العقوبة اثار قانونية بالغة الأهمية وهي :[٢٨٨]

أ.يمكن ملاحقة الفاعل جزائيا عن الشروع في الجريمة .

ب.أصبح بالمكان ترحيل فاعل الجريمة إلى دولة أخرى بناءا على طلبها إذا توفرت الشروط المتطلبة للترحيل .

ج. أصبحت هذه الجريمة من الجرائم التي يجوز التوقيف فيها .

وبعبارة موجزة إن هذه التعديلات وما ترتب عليها من اثار جعل القانون أكثر انسجاما مع الاتفاقية الاروبية الخاصة بالجريمة المعلوماتية لعام ٢٠٠١.

كما أن المشرّع البريطاني جرّم جريمة الدخول غير المصرح به إلى نظام معلومات بهدف ارتكاب جريمة أخرى في المادة الثانية من قانون اساءة استخدام الحاسوب البريطاني لعام ١٩٩٠ وتفرض هذه المادة عقوبة الحبس لمدة تصل إلى خمس سنوات . وتعتبر هذه الجريمة من الجرائم المركبة التي لا تشترط ارتكاب الجريمة الأخرى التي تم الدخول النظام المعلوماتي من اجلها. ولذلك تعتبر هذه الجريمة أكثر خطورة من الجريمة المنصوص عليها في الفقرة الأولى من فالقانون ذاته . وتشمل هذه المادة جميع الجرائم التي ورد النص عليها في التشريعات الجزائية مثل الاحتيال أو تلك الجرائم التي تعتبر من الجرائم القانون العام . وغاية ما في الأمر أن تكون الجريمة الأخرى من الجرائم التي يجوز التوقيف فيها سواء أكانت جناية أو جنحة .[٢٨٩]

كما جرّم المشرع الجزائي الانجليزي إتلاف عمل الحاسوب أو إعاقة الدخول إلى اي بيانات موضوعة في أي كمبيوتر أو إتلاف عمال أي برنامج أو تؤثر في صحة أي بيانات أو تحوير غير مصرح به بمعطيات الحاسوب بقصد إضعاف أو تعطيل النظام المعلوماتي بنص صريح في المادة الثالثة من قانون إساءة استخدام الكمبيوتر[٢٩٠] ولقد اختارت اللجنة القانونية المكلفة بوضع مشروع قانون إساءة استخدام الحاسوب اعتبار هذا الفعل جريمة قائمة بذاتها بدلا من الاعتماد على قانون ١٩٧١.

---

[288] سامي حمدان الرواشده/د.أحمد موسى الهياجنه، المرجع السابق ص١٣٢

[289] سامي حمدان الرواشده/د.أحمد موسى الهياجنه، المرجع السابق ص135

[290] سامي حمدان الرواشده/د.أحمد موسى الهياجنه، المرجع السابق 142

وقد تم تعديل المادة الثالثة من قانون إساءة استخدام الحاسوب بموجب المادة (٣٦) من قانون (police and Justice act 2006) [٢٩١] ومن أهم التعديلات التي نص عليها القانون الجديد زيادة العقوبة لتصبح لمدة ١٠ سنوات بدلا من٥ سنوات وأصبحت عقوبة الغرامة غير محددة،والهدف من التعديل هو التعامل مع ما يسمى (Denial of service attacks) أو أنشطة منع أو حجب الخدمة كخدمة الانترنت مثلا من خلال زيادة حمولة النظام المعلوماتي ومنع المستخدم من استعمال الخدمة عن طريق إرسال عدد كبير من الرسائل الالكترونية . إن تعديل نص المادة الثالثة جاء بهدف تحقيق انسجام بين قانون إساءة استخدام الحاسوب وبين المادة الخامسة من الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية والمادة الثالثة من قرار الاتحاد الأوروبي المتعلق بأنشطة الاعتداء على أنظمة معلوماتية ، ونتمنى على المشرع الأردني أن يسلك مسلك المشرع البريطاني وذلك بتعديل العقوبة الواردة في نص الفقرة (ب) من المادة الثالثة من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ إذا كان الهدف من الدخول غير المشروع إتلاف البيانات أو تعديلاها أو محوها .

المطلب الثاني : موقف بعض التشريعات العربية

اهتمام المشرع العربي بجريمة الإتلاف المعلوماتى لم يكن بذات المستوى الموجود لدى المشرع الغربي ، فأغلب الدول العربية لم تحرك ساكنا لمواجهة هذا النوع المستحدث من الجرائم إلا متأخرا واعتمدت على النصوص القائمة المنصوص عليها في مدوناتها العقابية ، ومع ذلك قامت بعض الدول العربية باستحداث نصوصاً خاصة بهذه الجرائم [٢٩٢]، والأمثلة التالية توضح ذلك

الفرع الأول: الموقف في التشريع العماني

يُعد القانون العماني أول قانون عربي[٢٩٣] يتطرق إلى مواجهة الإجرام السيبراني، من خلال التعديل الذي تم على قانون الجزاء العماني رقم ١٩٧٤/٧م، بموجب المرسوم السلطاني رقم ٢٠٠١/٧٢م، فجرم ١٠ صور جرمية في المادة ٢٧٦ مكررا هي: الالتقاط غير المشروع للمعلومات أو البيانات ، والدخول غير المشروع على أنظمة الحاسب الآلي ، و التجسس والتصنت على البيانات والمعلومات و انتهاك خصوصيات الغير أو التعدي على حقهم في

(291) سامي حمدان الرواشده/د.أحمد موسى الهياجنه، المرجع السابق ص144

(292) عبد الكريم خالد الشامي ،جرائم الكمبيوتر والانترنت في التشريع الفلسطيني ، مقال منشور في جريدة دنيا الوطن بتاريخ ٢٠١٠/٥/٢ http://pulpit.alwatanvoice.com/articles/2010/05/02/196865.html

(293) ناصر بن محمد البقمي – مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية الاربعاء ٩ رجب ١٤٣٠ هـ الموافق ١ تموز (يوليو) ٢٠٠٩ – مركز الإمارات للدراسات والبحوث الاستراتيجية، ط١، ٢٠٠٨م ص٤

الاحتفاظ بأسرارهم ، و تزوير بيانات أو وثائق مبرمجة أياً كان شكلها ، و إتلاف وتغيير ومحو البيانات والمعلومات ، و جمع المعلومات والبيانات وإعادة استخدامها و تسريبها ، و التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع ، و نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية.

المحاولة الثانية من محاولات المشرع العماني في التصدي لظاهرة الإجرام السيبراني جاءت من خلال قانون المعاملات الإلكترونية ٢٠٠٨ حيث جرم المشرع في المادتين (٥٢، ٥٣) بعض الأنماط السلوكية التي من شأنها هز ثقة الجمهور بالتعاملات التي تتم في العالم الرقمي حيث جرّم إتلاف المكونات المنطقية لأنظمة الحاسب الآلي بنص مستحدث خاص بها وهو نص البند الأول من المادة ٥٢ من قانون المعاملات الإلكترونية [٢٩٤] حيث نص على "" مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر ،يعاقب بالسجن لمدة لا تتجاوز سنتين و بغرامة لا تتجاوز ٥٠٠٠ ر٠ع (خمسة آلاف ريال عماني) أو بإحدى هاتين العقوبتين كل من : "تسبب عمداً في تعديل غير مرخص به في محتويات أي حاسب آلي بقصد إضعاف فاعليته أو منع أو تعويق الدخول إلى أي برنامج أو بيانات محفوظة فيه أو إضعاف فاعلية ذلك البرنامج أو إضعاف الاعتماد على تلك البيانات إذا تم ذلك التعديل بإحدى الطرق الآتية:

شطب أي برنامج أو بيانات محفوظة في الحاسب الآلي.

إضافة أي برنامج أو بيانات إلى محتويات الحاسب الآلي.

أي فعل يسهم في إحداث ذلك التعديل.

ويتضح لنا من خلال النص السابق أن السلوك الإجرامي يتحقق بالإتلاف ويعني بها إفناء هذه المعلومات وإهلاكها كليا أو جزئيا ، أو بالإضافة ويعني بها إضافة كلية أو جزئية للمحتويات الموجودة في الحاسب الآلي وهاتين الصورتين وردتا على سبيل المثال وليس الحصر بدليل أن المشرع أورد في نهاية البند عبارة (أي فعل يسهم في إحداث ذلك التعديل) .هذا من ناحية ومن ناحية أخرى نجد أن المشرّع العماني وهو يجرم هذه الجريمة لم يحدد الجهة التي تتبع لها البيانات فهو لم يضع شروطا تتعلق بطبيعة البيانات و المعلومات محل الإتلاف ولم يشترط تبعيتها لجهة

(294) المشرع العماني أيضا جرم الإتلاف المعلوماتي بنص آخر وهو نص البند السادس من المادة ٢٧٦مكرر من قانون الجزاء العماني حيث نص على « يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين وبغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب إحدى الأفعال التالية :..... ٦- إتلاف وتغيير ومحو البيانات والمعلومات.«

معينة وإنما جاء النص عاما ليشمل كافة أنواع المعلومات والبيانات سواء أكانت تابعة لجهة حكومية أو خاصة ، ومن ناحية ثالثة لم يحدد وسائل معينة تتم بها عملية الإتلاف المعلوماتي ، مما يعني أن النص يتسع ليشمل كافة الطرق الفنية والتقنية المستخدمة في إتلاف المعلومات بما في ذلك استخدام البرامج الخبيثة كالفيروسات والقنابل المعلوماتية وبرامج الدودة وغيرها ، ومن ناحية رابعة نجد أن الجريمة تقوم بمجرد القيام بأحد الأفعال الإجرامية كما وأن العقاب على إتلاف المعلومات لم يرتبط بالدخول غير المصرح به إلى نظام الحاسب الآلي.

وتناول المشرع العماني جريمة الاختراق المعلوماتي(٢٩٥) كونها تعد من أخطر الجرائم التي تهدد المعلوماتية ، من هذا المنطلق نجد أن المشرع العماني كان حريصا على تجريم هذه الفئة المستحدثة من الجرائم بنصوص خاصة أوردها في المادة ٥٢ من قانون المعاملات الالكترونية وهذه النصوص هي نص البند الثاني ونص البند الثالث عشر وذلك على النحو التالي النحو التالي

١. النص الوارد في البند الثاني :

"اخترق جهاز حاسب آلي أو منظومة حاسبات آلية أو موقع على الإنترنت أو شبكة الإنترنت وترتب على ذلك:

أ. تعطيل أنظمة تشغيل جهاز الحاسب الآلي أو منظومة الحاسبات الآلية.

ب. إتلاف برامج الحاسب الآلي أو الحاسبات الآلية وما تحتويه من معلومات.

ج. سرقة المعلومات.

د. استخدام المعلومات التي تتضمنها مخرجات الحاسبات الآلية في أغراض غير مشروعة

ه. إدخال معلومات غير صحيحة

والاختراق المعاقب عليه وفقا لهذه المادة هو الاختراق الذي يترتب عليه نتيجة معينة ، بمعنى أن الجريمة لا تقوم إلا إذا ترتب على الفعل الإجرامي إحدى النتائج التالية : تعطل النظام أو الموقع المخترق ،إتلاف البرامج الحاسوبية أو أجهزة الحاسب الآلي أو المعلومات التي عليه ، سرقة المعلومات التي في النظام أو الموقع المخترق أو استخدامها بصورة غير مشروعة ، إدخال معلومات غير صحيحة .

وحقيقة الأمر نجد أن المشرع في هذه النقطة الأخيرة قد جانبه الصواب فكان الأحرى به تجريم الاختراق المجرد بمعني أن الجريمة تقوم بمجرد الدخول الغير مشروع إلى النظام سواء ترتب

(295) سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت ""دراسة مقارنة"" ، دار النهضة العربية-القاهره، ٢٠٠٩ ،ط ١ ، ص٣٣٥

على هذا الدخول ضرر أو نفع . أيضا نجد أن المشرع العماني ومن جانب أخر لم يتطرق إلى تجريم البقاء غير المشروع داخل أنظمة الحاسب الآلي فيما لو تم الدخول سهوا أو دون قصد على الرغم من أن الفعل لا يختلف عن الدخول غير المشروع من حيث وجوب التجريم فاتجاه إرادة الفاعل في البقاء داخل النظام على الرغم من معرفته أنه غير مصرح له بالدخول إليه لا يختلف في جوهره عن الدخول غير المصرح به إلى أنظمة الحاسب الآلي ، فالنتيجة الإجرامية واحدة في هاتين الحالتين وهي الوصول إلى النظام الآلي.

٢.النص الوارد في البند الثالث عشر :

الدخول غير المشروع إلي حاسب آلي بقصد ارتكاب جريمة أو تسهيل ارتكاب جريمة سواء بواسطته أو بواسطة شخص آخر .

ومن منطلق رغبة المشرع العماني في سد النقص التشريعي في هذا المجال ، وكون النصوص الواردة في سلسلة التشريعات السالف ذكرها لم تعد كافية لمواجهة هذه النوعية من الجرائم. تم صدور قانون مكافحة جرائم تقنية المعلومات ٢٠١١/١٢في الربع الأول من عام ٢٠١١ بموجب المرسوم السلطاني ٢٠١١/١٢ . تناول الفصل الثاني من القانون جرائم الاعتداء على سرية وسلامة وتوافر البيانات والمعلومات وإساءة استخدام الأدوات فجرم في المادة الثالثة منه: ثلاثة أفعال هي الدخول غير المشروع ، وتجاوز الدخول المصرح به ، والبقاء غير المشروع ، على المواقع والأنظمة الإلكترونية ، وفرض عقوبة السجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال و لا تزيد على خمسمائة ريال أو بإحدى هاتين العقوبتين[٢٩٦].

فإذا ترتب على ما ذكر في الفقرة الأولى؛ إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات؛ أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية؛ أو إلحاق ضرر بالمستخدمين أو المستفيدين، تكون العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال ولا تزيد على ألف ريال أو بإحدى هاتين العقوبتين . أما إذا ترتب على الأفعال السابقة ؛ إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل

---

(296) سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت ""دراسة مقارنة"" ، دار النهضة العربية-القاهره، ٢٠٠٩ ،ط ١ ، ص٣٣٥

تقنية المعلومات؛ أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية؛ أو إلحاق ضرر بالمستخدمين أو المستفيدين، تكون العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال ولا تزيد على ألف ريال أو بإحدى هاتين العقوبتين(٢٩٧) .

الفرع الثاني : التشريع السعودي

أورد النظام السعودي لسنة ١٤٢٨ هـ (٢٠٠٧ م.) (٢٩٨)جريمة العبث بالنظام في شكل إيقاف عمله أو تعطيله أو تدميره أو مسح البرامج. وكذلك تشمل الجريمة العبث بالبيانات وذلك في شكل إتلافها أو تعديلها أو تسريبها، وذلك بنصه في المادة الخامسة: "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين ، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت."

وواضح من اتجاه التشريع السعودي أنه تمشى مع الاتجاه الحديث في ضرورة إيجاد نص خاص للعقاب على إلغاء أو إتلاف البيانات وعدم ترك الأمر للقواعد العامة التي يختلف فيها الرأي حول ما إذا كان التجريم الخاص بالإتلاف الموجود في كثير من التشريعات يسري على البيانات مثلها في ذلك مثل غيرها من المنقولات أي هل البيانات والبرامج هي من قبيل المنقولات التي يحميها تجريم إتلاف المنقولات؟ وقد أحسن التشريع السعودي بإيراده نص خاص للعقاب على إتلاف وحذف البيانات والبرامج(٢٩٩).

المبحث الرابع :القواعد العامة للمسئولية لجريمة الدخول غير المشروع لنظام معلومات والتطبيقات القضائية

(297) سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت ""دراسة مقارنة"" ، دار النهضة العربية-القاهره، ٢٠٠٩ ،ط ١ ، ص٣٣٥

(298) قانون نظام مكافحة جرائم المعلوماتية السعودي-الصادر بالمرسوم الملكي السعودي رقم م/ ١٧ بتاريخ ٢٧ أبريل ٢٠٠٨- منشور على موقع الموسوعة الحرة "جوريسبيدياwww.jurispidia.com "

(299) شيماء عبد الغني محمد عطا الله مكافحة جرائم المعلوماتية في المملكة العربية السعودية بحث منشور http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx#_ftn4: 21/11/2011

إن دراسة أي جريمة من الناحية القانونية وفق النص الذي تستند إليه لا بد من الأخذ بعين الاعتبار جميع النصوص الواردة في القانون المختص من ناحية التبرير والتشديد والإباحة والاختصاص وعليه سوف نتناول القواعد العامة للمسؤولية عن الدخول غير المشروع كمطلب أول والتطبيقات القضائية كفرع ثاني رغم ندرتها

المطلب الأول القواعد العامة للمسئولية عن جريمة الدخول غير المشروع لنظام معلومات

أورد قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ في المملكة الأردنية الهاشمية من النصوص ما يبين الخطوط العامة للمسئولية عن جرائم المعلوماتية وخاصة فيما أورده من أحكام موضوعية للمسئولية الجنائية عن جرائم المعلوماتية على الوجه التالي:

أولا- الجمع بين عقوبات أصلية وعقوبات تكميلية

العقوبة الأصلية تعتبر في نظر الشارع كافية لتحقيق معنى الجزاء المقابل للجريمة وقد عرفتها محكمة النقض المصرية قائلة)((إن العقوبة تعتبر أصلية إذا كونت العقاب المباشر للجريمة ووقعت منفردة دون ان يعلق القضاء بها على حكم بعقوبة أخرى)[٣٠٠] وهي :

الإعدام والإشعال الشاقة بنوعيها والاعتقال بنوعيه والحبس وكذلك تعتبر أصلية الغرامات والعقوبات المقررة للمجرمين الأحداث لأنه يحكم بها بمفردها .

وقد تكون العقوبة تكميلية أو اضافيه وهي جزاء ثانوي للجريمة تستهدف الجزاء الكامل لها وهي مرتبطة بالجريمة دون عقوبتها الأصلية وقد تكون وجوبية أو جوازية[٣٠١].

و قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ يجمع بين عقوبات أصلية. حيث قرر القانون عقوبة الحبس وقرر عقوبة الغرامة مع السجن جوازية للمحكمة بقوله "أو بكلتا هاتين العقوبتين". فقد خول القانون المحكمة في جريمة الدخول غير المشروع لنظام معلومات أو موقع الكتروني سلطة الحكم بعقوبة الحبس أو الغرامة؛ فإن قضت المحكمة بأحدهما كانت عقوبة أصلية، كما أجاز للمحكمة أن تحكم بالغرامة بالإضافة إلى الحبس؛ مثال ذلك المادة٣- أ- كل من دخل قصداً إلى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو

---

(300) كامل السعيد ، المرجع السابق صفحه ٦٤٩

(301) نظام توفيق المجالي، المرجع السابق ، صفحة ٦٤٩ و٦٥٠

يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٢٠٠) مائتي دينار أو بكلتا هاتين العقوبتين .

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفتـــــــه أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار أو بكلتا هاتين العقوبتين.

وتدرج المشرع الأردني في قانون جرائم أنظمة المعلومات لعام ٢٠١٠ في العقوبة من الحبس أو الغرامة إلى الإشغال الشاقة ، حيث شدد العقوبة إذا كان الهدف من الدخول غير المشروع إتلاف البيانات أو تعديلها أو بهدف استخدام بطاقة الائتمان للغير أو الترويج للدعارة أو التجسس أو القيام بأعمال إرهابية وأشارت إلى ذلك المواد ٣، ٤ ، ٥، ٦، ٨،٩، ١٠، ١١) من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ .[٣٠٢]

ثانيا- التخيير بين عقوبة الغرامة وعقوبة الحبس

قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ قرر عقوبة مرتفعة في حدها الأقصى وهو الإشغال الشاقة المؤقتة في المواد (١١ و١٠ و ٨) من قانون جرائم أنظمة المعلومات لعام ٢٠١٠، لكنه راعى في نفس الوقت أن يكون هناك حدا أدنى منخفض يتمثل في أنه أورد عقوبة الغرامة (١٠٠ دينار أو ٢٠٠ ..) في جريمة الدخول المجرد غير المشروع لنظام معلومات أو موقع الكتروني. والحد الأدنى لعقوبة السجن مدة لا تقل عن أسبوع في جريمة الدخول المجرد غير المشروع ، مادامت الجريمة لم يتوافر فيها ظرف مشدد حسب المادة ٣/أ من قانون جرائم أنظمة المعلومات لعام ٢٠١٠. ويدل ذلك على رغبة المشرع في زيادة السلطة التقديرية للقاضي الجزائي حتى يواجه فروضا عديدة يضيق عنها أي تعداد.

ومن الجدير بالذكر أن المشرع الأردني يجيز في تنفيذ الأحكام أن يُستبدل الحبس بالغرامة، عن كل يوم حبس دينارين حسب المادة ٢٧ من قانون العقوبات الأردني [٣٠٣]ويجوز أن تُستبدل

---

[302] قانـــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

[303] المادة (٢٧) من قانون العقوبات الاردني

٢. إذا حكم على شخص بالحبس مدة لا تزيد على ثلاثة أشهر يجوز للمحكمة التي أصدرت الحكم أن تحوّل مدة الحبس إلى الغرامة على

الغرامة بالحبس بالشروط والقيود التي يُبينها القانون ،حسب المادة ٢٢ من قانون العقوبات الأردني [٣٠٤] .

ثالثا – تقرير المصادرة كعقوبة تكميلية جوازيه

أورد قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ عقوبة المصادرة وعقوبة الإغلاق بوصفهما عقوبتين تكميليتين يكون الحكم يهما جوازيا للمحكمة بنصه في المادة الثالثة عشرة من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ (١١-ج- للمحكمة المختصة الحكم بمصادرة الأجهزة و الأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة مرتكب الجريمة.

رابعا- تشديد العقاب عند توافر بعض الظروف المشددة

تقسم الظروف المشددة إلى عدة أقسام منها ما يتعلق بالركن المادي أو المعنوي وتنقسم إلى ظروف مادية وظروف شخصية ، والظروف المادية تتعلق بالركن المادي للجريمة وتشمل ما يتصل بالسلوك الجرمي أو نتائجه كالتسور والإكراه في السرقة أو ظرف الليل ، أما النتائج المترتبة على هذا السلوك فتعد ظروف مشددة كحدوث الموت أو العاهة الدائمة كأثر لفعل أو الجرم المقصود ،أما الظروف المشددة الشخصية فتتعلق بالجانب المعنوي للجريمة أو بالشخصية مثل سبق الإصرار في القتل العمد (مادة ٣٢٨ عقوبات أردني) .[٣٠٥]

أورد قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ بعض الظروف التي من شأنها أن تشدد العقاب عن العقوبة الأصلية المقررة لمرتكب الدخول المجرد غير المشروع لنظام المعلومات، حيث شدد العقوبة في حال كان الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات بهدف إتلاف البيانات أو تعديلها في المواد ٣/ب و٤ من القانون ذاته وكذلك شدد العقوبة في حال ارتكاب الجرائم المنصوص عليها في المواد من ٣الى ٦ من قانون جرائم أنظمة

أساس دينارين عن كل يوم وذلك إذا اقتنعت بان الغرامة عقوبة كافية للجريمة التي أدين بها ذلك الشخص.

([304]) المادة (٢٢) من قانون العقوبات الاردني

الغرامة ، هي إلزام المحكوم عليه بأن يدفع الى خزينة الحكومة المبلغ المقدر في الحكم ، وهي تتراوح بين خمسة دنانير ومايتي دينار إلا إذا نص القانون على خلاف ذلك:

١. اذا لم يؤد المحكوم عليه بالغرامة المبلغ المحكوم به عليه ، يحبس في مقابل كل دينارين او كسورهما يوماً واحداً على أن لا تتجاوز مدة الحبس في هذه الحالة سنة واحدة.

([305]) نظام المجالي ، المرجع السابق ، صفحه ٤٣٩

المعلومات لعام ٢٠١٠ إذا ارتكبها شخص أثناء تأديته للوظيفة أو قام باستغلالها وهذا ما نصت عليه المادة ٧ بـــــ:

(المادة٧- تضاعـــــف العقوبة على الجرائم المنصوص عليها في المواد من (٣) إلى (٦) من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأديته وظيفته أو عمله أو باستغلال أيٍ منهما.

وكذلك شدد المشرع الأردني في قانون جرائم أنظمة المعلومات لعام ٢٠١٠ العقوبة إذا كان الدخول إلى موقع الكتروني أو نظام معلومات بهدف الاطلاع على معلومات تمس الأمن القومي أو إتلافها وذلك بنص المادة ١١ :

(المادة ١١-أ- كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع الكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامـــــة أو الاقتصـــــاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٥٠٠٠) خمسة ألاف دينار).

التكرار ظرف مشدد عام بالنسبة للجنايات والجنح دون المخالفات حيث أورد المشرع الأردني في الأحكام الخاصة بالتكرار في المواد (١٠١-١٠٤) من قانون العقوبات الأردني .[٣٠٦]

والمشرع الأردني في قانون جرائم أنظمة المعلومات لعام ٢٠١٠ قام بتشديد العقوبة في حالة تكرار أي من الجرائم المنصوص عليها في هذا القانون ، حسب نص المادة ١٥من قانون جرائم أنظمة المعلومات حيث نصت على ما يلي :

(المادة ١٥- تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم المنصوص عليها فيه)

خامسا – العقاب على الشروع

لم يعاقب قانون جرائم المعلوماتيه الأردني على الشروع في جريمة الدخول غير المشروع لنظام معلومات بهدف إتلاف أو محو أو تعديل البيانات.

بينما نجد أن التشريع السعودي (في نظام مكافحة جرائم المعلوماتية لعام ٢٠٠٧) يعاقب على جريمة الشروع في جميع جرائم المعلوماتية بنص واضح، فتنص المادة العاشرة على أنه "يعاقب

---

[306] نظام المجالي ، المرجع السابق ، صفحه ٤٤٠

كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة."

سادسا - العقاب على الاشتراك في جرائم المعلوماتية:

عالج المشرع الأردني حالة تعدد الشركاء (الشركاء الأصليين) الذين يقومون بادوار رئيسية في الجريمة في المادتين (٧٥، ٧٦) من قانون العقوبات الأردني ، فالصورة الأول عبّر عنها المشرع للفاعل في المادة ٧٥ بقوله... (من ساهم مباشرة في تنفيذها) ، أما الصورة الثانية فقد نصت عليها المادة ٧٦ من القانون ذاته بقوله (إذا ارتكب عدة أشخاص متحدين جناية أو جنحة ، أو كانت الجناية أو الجنحة تتكون من عدة أفعال فأتى كل واحد منهم فعلا أو أكثر من الأفعال المكونة لها وذلك بقصد حصول تلك الجناية أو الجنحة اعتبروا جميعهم شركاء فيها وعوقب كل واحد منهم بالعقوبة المعينة لها في القانون ، كما لو كان فاعلاً مستقلا لها) . وعند استقراء هذا النص نستنبط أن الشريك الأصلي يعاقب بنفس العقوبة كما لو كان فاعلا مستقلا للجريمة . والمشرع الأردني في قانون الجرائم أنظمة المعلومات لعام ٢٠١٠ سلك نفس النهج في معاقبة الشريك الأصلي وعاقبه كما لوكان مرتكب الجريمة المعلوماتية فاعلا مستقلا حيث أشارت المادة ١٣ من قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ (١٣- يعاقب كل من قام قصداً بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها) .

والملاحظ أن المشرع الأردني في قانون جرائم أنظمة المعلومات لعام ٢٠١٠ساوى في العقوبة بين الفاعل المستقل والشريك الأصلي والمحرض والمتدخل في العقوبة بنص المادة ١١ السالفة الذكر ويكون بذلك خالف سياسية المشرع الأردني في قانون العقوبات بالنسبة للمتدخل والمحرض وتماشى معه بالنسبة للشريك الأصلي ، حيث عاقبت المادة (٨٠ ، ٨١) من قانون العقوبات الأردني المحرض والمتدخل بعقوبة اقل من الفاعل المستقل والشريك الأصلي بقولها :

المحرض والمتدخل

المادة (٨٠)

١-أ- يعد محرضاً من حمل أو حاول أن يحمل شخصاً آخر على ارتكاب جريمة بإعطائه نقوداً أو بتقديم هدية له أو بالتأثير عليه بالتهديد أو بالحيلة والخديعة أو باستغلال النفوذ أو بإساءة الاستعمال في حكم الوظيفة.

ب- إن تبعة المحرض مستقلة عن تبعة المحرض على ارتكاب الجريمة.

٢- يعد متدخلاً في جناية أو جنحة.

أ- من ساعد على وقوع جريمة بإرشاداته الخادمة لوقوعها.

ب- من أعطى الفاعل سلاحاً أو أدوات أو أي شيء آخر مما يساعد على إيقاع الجريمة.

ج- من كان موجوداً في المكان الذي ارتكب فيه الجرم بقصد إرهاب المقاومين أو تقوية تصميم الفاعل الأصلي أو ضمان ارتكاب الجرم المقصود.

د- من ساعد الفاعل على الأفعال التي هيأت الجريمة أو سهلتها أو أتمت ارتكابها.

هـ- من كان متفقاً مع الفاعل أو المتدخلين قبل ارتكاب الجريمة وساهم في إخفاء معالمها أو تخبئة أو تصريف الأشياء الحاصلة بارتكابها جميعها أو بعضها أو إخفاء شخص أو أكثر من الذين اشتركوا فيها عن وجه العدالة.

و- من كان عالماً بسيرة الأشرار الجنائية الذين دأبهم قطع الطرق وارتكاب أعمال العنف ضد أمن الدولة أو السلامة العامة ، أو ضد الأشخاص أو الممتلكات وقدم لهم طعاماً أو مأوى أو مخبأ أو مكاناً للاجتماع.

المادة (٨١)

يعاقب المحرض أو المتدخل:

١- أ- بالأشغال الشاقة المؤقتة من خمس عشرة سنة إلى عشرين سنة إذا كانت عقوبة الفاعل الإعدام.

ب- بالأشغال الشاقة المؤقتة من سبع سنوات إلى خمس عشرة سنة إذا كانت عقوبة الفاعل الأشغال الشاقة المؤبدة أو الاعتقال المؤبد

٢- في الحالات الأخرى ، يعاقب المحرض والمتدخل بعقوبة الفاعل بعد أن تخفض مدتها من السدس إلى الثلث.

٣- اذا لم يفض التحريض على ارتكاب جناية او جنحة الى نتيجة خفضت العقوبة المبينة في الفقرتين السابقتين من هذه المادة الى ثلثها.

سابعا- عدم تنظيم مسئولية مزودي الخدمات:

لم يرد في قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ نصوص تعالج مسئولية مزودي الخدمات، فهل يسألون عما يقومون ببثه من مواد على شبكة الانترنت ؟ هل هذه المسئولية مطلقة

؟ هل هي مشروطة بشروط معينة؟ ما هي مسئولية مالك الموقع ؟ نتمنى على المشرع الأردني معالجة ذلك حتى لا يفلت مجرم من العقاب.

ثامنا – عدم تقرير مسئولية الشخص المعنوي:

لم يعالج المشرع الأردني في قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ مسئولية الشخص المعنوي كالشركات مثلا إذا وقعت جريمة من الجرائم المشار إليها في القانون عن طريق ممثل الشركة أو أحد العاملين لحسابها أو أحد مستخدميها. فهل يمكن حل الشركة ؟ هل يمكن قفل المنشأة ؟ هل يمكن فرض غرامة على الشركة؟

تاسعا – التعويض الشخصي

يجوز إقامة دعوى الحق الشخصي أي دعوى المطالبة بالتعويض عما لحق بالضحية أو المجني عليه من ضرر مادي أو نفسي أو معنوي تبعا لدعوى الحق العام ، وقد أشارت إلى ذلك المادة (١/٦) من قانون أصول المحاكمات الجزائية الأردني .

المشرع الأردني في قانون جرائم أنظمة المعلومات لعام ٢٠١٠ أعطى الحق للمتضرر ان يقيم دعوى الحق العام والحق الشخصي أمام القضاء المختص إذا ارتكبت إحدى الجرائم المنصوص عليها في القانون ذاته وذلك بحسب نص المادة ١٦ من قانون جرائم أنظمة المعلومات لعام ٢٠١٠ والتي نصت على ما يلي :

(المادة ١٦- يجوز إقامة دعوى الحق العام والحق الشخصي على المشتكى عليه أمام القضاء الأردني إذا ارتكبت أياً من الجرائم المنصوص عليها في هذا القانون باستخدام أنظمة معلومات داخل المملكة أو ألحقت أضرارا بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها ، كليا أو جزئيا ، أو ارتكبت من أحد الأشخاص المقيمين فيها).

المطلب الثاني : تطبيقات قضائيه

وفي هذا المطلب سوف نطرح قضايا تطبيقة لجريمة الدخول غير المشروع لنظام معلومات ورغم ندرتها إلا أننا اجتهدنا في طرح بعض التطبيقات القضائية في كل من بريطانيا وفي بعض الدول العربية الشقيقة .

جريمة الدخول غير المشروع (القضاء البريطاني)

ومن الجدير بالذكر أن القضاء البريطاني اصدر عددا من الأحكام القضائية أثبتت فاعلية قانون إساءة استخدام الحاسوب للتصدي إلى مرتكبي هذا النوع من الجرائم خاصة أولئك الذين يحاولون الدخول إلى نظام حاسب الآلي من بعد باستخدام نظام معلوماتي اخر ويتجلى ذلك بكل وضوح بالقرار القضائي التي أصدرته إحدى المحاكم الانجليزية والقاضي بإدانة الشاب البريطاني بالجريمة المنصوص عليها في المادة الأولى من قانون إساءة استخدام الحاسوب بعد ان تمكن من خرق النظام المعلوماتي الخاص بوزارة الدفاع الأمريكي[٣٠٧] ومما لاشك في أن هذا القرار يؤكد نجاح القانون في تحقيق الهدف الذي سن من اجله .

وفي قضية أخرى تتخلص وقائعها بقيام المدعوة (Ojomo) التي كانت تعمل بوظيفة محللة مالية في شركة American Express بالدخول إلى كافة حسابات العملاء على الرغم من أنها كانت مخولة للدخول على بعض الحسابات، وتمكنت من الحصول على معلومات سرية من هذه الحسابات وإعطائها لشخص يدعى(Allison) ، وتم استخدام هذه المعلومات للحصول على الأرقام السرية للحسابات وبعض بطاقات الائتمان ثم استخدمت هذه المعلومات للاستيلاء على مبالغ نقدية كبيرة من أجهزة الصراف الآلي .عند اكتشاف الأمر قررت محكمة الجزاء الابتدائية ان الفعل الذي قامت به(Ojomo)لا يشكل انتهاكا لنص المادة الأولى من قانون إساءة استخدام الكمبيوتر في ظل القرار الصادر في قضية (Bignell) وقد تم تأييد هذا القرار من قبل محكمة الاستئناف، ولكن تم الطعن في هذا القرار لدى مجلس اللوردات وكان السؤال المطلوب الإجابة عليه هو هل يمكن للموظف المخول الدخول للمعلومات المختزنة في النظام المعلوماتي ان يرتكب جريمة الدخول غير المصرح به خلافا لأحكام المادة الأولى؟

قرر مجلس اللوردات إن سلوك (Ojomo) يشكل جريمة الدخول غير الصرح به التي يعاقب عليها بموجب أحكام المادة الأولى من قانون إساءة استخدام الحاسوب .وذلك لأنها استخدمت نظام الحاسوب للحصول على معلومات لم تكن مخولة للدخول لها أو انها لم تحصل على تصريح لازم للدخول إلى تلك المعلومات، فكلمة تحكم"control"لا يقصد بها القدرة على تشغيل جهاز الحاسوب فقط. ان المادة (١١٧\٥) من قانون اساءة استخدام الحاسوب تعني ان صلاحية الدخول إلى نوع معين من المعلومات لا يعطي الصلاحية للدخول إلى معلومات أخرى حتى ولو كانت من ذات

---

[307] R.v.Pryce(Unreported, Bow Street Magistrates, March,21,1997 .

انظر كذلك : سامي حمدان الرواشده ،.أحمد موسى الهياجنه، المرجع السابق ، ص ١٤٦

الصنف ، فالمادة الأولى من القانون تشير إلى إرادة الدخول إلى النظام المعلوماتي دون تصريح ، بعد أن استعرض مجلس اللوردات تقرير اللجنة القانونية التي أعدت والتي بينت أن القانون يهدف إلى معاقبة هؤلاء المخولين بالدخول إلى النظام المعلوماتي ويسيئون استخدامه خلص إلى نتيجة مفادها إن التفسير الضيق لنصوص القانون من شانه أن يفوت الغاية من إصدار القانون ويحد من فاعليته في التعامل مع الصور المختلفة لآساءة استخدام الحاسوب. والقرار الصادر من مجلس اللوردات عالج ثغرة قانونية يمكن ان يترتب عليها أن تبقي الوقائع السابقة خارج نطاق التجريم[٣٠٨] .ويرى الفقه ان منهج مجلس اللوردات عقلاني وعملي لأنه يضع بصورة ضمنية وقواعد قانونية تنسجم مع المعاير الاجتماعية والتجارية على حد سواء.[٣٠٩]

جريمة الدخول غير المشروع (القضاء الإماراتي) :

تتلخص وقائع هذه القضية بأن المتهم توصل وبغير وجه حق إلى الدخول على جهاز الحاسب للمجني عليها ونسخ البيانات والمعلومات الشخصية الخاصة بها.

هدد المتهم المجني عليها بواسطة الشبكة المعلوماتية بأنه سيقوم بنشر صورها عبر فضاء الانترنت إذا لم تضيفه إلى قائمة أصدقائها في برنامج المحادثة المرئية والمسموعة " الماسنجر. "

طالبت النيابة العامة بمعاقبة المتهم طبقا لأحكام المواد ٩،٢،٢٥،١ من القانون الاتحادي الإماراتي في شأن مكافحة جرائم تقنية المعلومات .

حكمت المحكمة حضوريا بمعاقبة المتهم بالحبس لمدة ستة أشهر مع احتساب مدة التوقيف وإبعاده عن الدولة ومصادرة جهاز الحاسوب المضبوط.[٣١٠]

جريمة الدخول غير المشروع بهدف الاستيلاء على أموال الغير (ا ماراني)

وقعت هذه الجريمة في شهر يونيو من هذا العام ٢٠٠٦ بدبي وقدمت النيابة العامة اثنين من المتهمين فيها للمحاكمة، وهي أول جريمة تقدم استنادا لقانون تقنية جرائم المعلومات لعام ٢٠٠٦ بدولة الإمارات ويدان مرتكبها،واتهمت النيابة العامة بدبي المتهم الأول بأنه ((توصل عن طريق

---

[308] KEIIY Stein ,"Unauthorized Access and the Computer Misuse Act 1990: House of Lords Leaves no Room for Ambiguity" 2000 Computerand Telecommmunications Law Review 6/3,63-66

انظر كذلك : سامي حمدان الرواشده ،.أحمد موسى الهياجنه، المرجع السابق ، ص ١٤٩ و١٥٠

[309] سامي حمدان الرواشده ،.أحمد موسى الهياجنه، المرجع السابق ، ص ١٥٠

[310] القضية رقم ٥٠٤٤ لسنة ٢٠٠٩ – محكمة العين الابتدائية أنظر المستشار الدكتور : محمد محمود الكمالي ، ورقة بحثية حول بعض قضايا جرائم تقنية المعلومات من محاكم دولة الامارات العربية المتحدة ، المؤتمر الإقليمي الأول ٢٥ اكتوبر ٢٠١٠ عمان الأردن. - لحماية برنامج الحاسوب وجرائم الانترنت – ٢

الشبكة المعلوماتيه إلي الاستيلاء على مال منقول (عدد خمس تذاكر سفر)عائد لشركة سفريات وسياحة بدبي بطريقة احتيالية وباتخاذ صفة غير صحيحة بأن تمكن من دخول موقع الشركة الإلكتروني عن طريق استخدام الرقم السري واسم المستخدم (الخاصين بالمتهم الثاني) وهو أحد موظفي الشركة وكان ذلك من شأنه خداع الشركة وحملها على تسليم تذاكرالسفر.

واتهمت النيابة الثاني بأنه اشترك بالاتفاق والمساعدة مع المتهم الأول بارتكاب الجريمة المبينة في الوصف السابق فوقعت الجريمة بناء على ذلك الاتفاق والمساعدة.

كما اتهمته بأنه بحكم عمله لدى الشركة بمهنة بائع تذاكر أفشى سر مهنته (الرقم السري واسم المستخدم) في غير الأحوال المصرح بها قانونا واستعمله لمصلحته الخاصة ومصلحة المتهم الأول دون إذن من صاحب الشأن.

وطلبت النيابة عقابهما بالمواد (١،١٠،٢٣،٢٥) من القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات والمادة ٣٧٩ من قانون العقوبات الاتحادي.

وقد دافع المتهم الأول عن التهمة الموجهة له بأنه لم يكن يقصد الاحتيال وقد ردت المحكمة هذا الدفاع بأن المتهم قد اتفق مع المتهم الثاني الموظف بالشركة الهارب وحصل منه على الرقم السري واسم المستخدم، وقام في أزمنة مختلفة باستخدامها عن طريق الدخول على موقع الشركة وتمكن من الحصول على التذاكر باعترافه، مع انه ليس له صفة الدخول ولايحق له استخدام الرقم السري واسم المستخدم مما يشكل فعله طريقة إحتياليه باتخاذ صفة غير صحيحة ليتمكن من الدخول للموقع وكان من شان ذلك خداع الشركة وحملها على تسليم تذاكر السفر المبينة بالأوراق.

وقد ادانتهما المحكمة طبقا للمادة ٢١٢ من قانون الإجراءات الجزائية والمواد ١،١٠،٢٣،٢٥) من قانون جرائم تقنية المعلومات والمادة ٣٧٩ من قانون العقوبات وحكمت على المتهم الأول بالحبس لمدة شهرين وإبعاده عن البلاد. وحكمت على المتهم الثاني بالحبس لمدة سنة واحدة وإبعاده عن البلاد. وقد أعملت المحكمة قواعد الارتباط المقررة في القانون بالنسبة للتهم الموجهة للمتهم الثاني وعاقبته بالعقوبة المقررة للجريمة الأشد، كما انها طبقت أحكام المواد ٩٩ ، و ١٠٠ من قانون العقوبات وعاملت المتهم الأول بقسط من الرأفة لظروف الدعوى وتنازل المجني عليها (الشركة).[٣١١]

---

(311) انظر الحكم الصادر من من محكمة التمييز بدبي بجلسة ٢٠٠١/١٢/٨ في القضية رقم ٢٠٠١/٢٣٠

جريمة الدخول غير المشروع : (القضاء العماني)[٣١٢]

من التطبيقات القضائية العمانية قضية تتلخص وقائعها في قيام مجموعة من الأشخاص الأجانب بالاستيلاء غير المشروع على بيانات ومعلومات خاصة بالبطاقات المالية لعملاء بعض البنوك العاملة بالسلطنة وذلك باستخدام أجهزة الحاسب الآلي وبعض الأجهزة المساعدة

ذهبت سلطة الاتهام بعد التحقيق في القضية إلى أن الواقعة تشكل بحق المتهمين جنحتي استخدام الحاسب الآلي عمدا في الالتقاط غير المشروع للمعلومات ، والاستيلاء على نحو غير مشروع على بيانات تخص الغير . وطالبت بإدانتهم ومعاقبتهم بموجب المادتين ٢٧٦ مكرر[٣١٣] والمادة ٢٧٦مكرر ١[٣١٤] ، كما طالبت بتشديد العقوبة بحق المتهمين كونهم من مستخدمي الحاسب الآلي وذلك عملا بنص المادة ٢٧٦مكرر ٢[٣١٥] من ذات القانون.

وعند عرض القضية على القضاء قرّرت الدائرة الجزائية بالمحكمة الابتدائية، بعد عدة جلسات ، وبحق إلى أن الأفعال المرتكبة من قبل المتهمين كانت لتنفيذ خطة إجرامية واحدة وبالتالي فهي تشكل تعدد معنويا وقضت بعقوبة الوصف الأشد عملا بنص المادة ٣١ من قانون الجزاء العماني[٣١٦] ، أما فيما يتعلق بتشديد العقوبة فذهبت المحكمة إلى أن لفظ (مستخدمي) الواردة في (المادة ٢٧٦مكرر ١) تشمل مدلول أوسع من لفظ (استخدام) ، فالأولى تعني التمرس والاحتراف وتعدد الاستخدام وكثرته ، بينما مدلول الثانية هو استخدام الحاسب الآلي على نحو عابر دون الاحتراف ، وبما أن سلطة الاتهام لم تقدم لها ما يفيد اعتياد المتهمين على استخدام الحاسب الآلي فإنها تستبعد استعمال(المادة ٢٧٦مكرر ١) بحق المتهمين. وحكمت بادنتهم جميعا بتهمة استخدام الحاسب الآلي عمدا في الالتقاط غير المشروع للمعلومات والاستيلاء على نحو غير مشروع على بيانات تخص الغير وقضت بسجنهم لمدة سنتين مع طردهم من البلاد مؤبدا بعد انتهاء فترة عقوبتهم ومصادرة الأدوات المضبوطة التي كانت بحوزتهم .

---

(312) قضية رقم ٣/ق/٢٠٠٤ الدائرة الجزائية – المحكمة الإبتدائية مسقط.

(313) تنص هذه المادة على: ""يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين وبغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الأفعال الآتية: ١ .الالتقاط غير المشروع للمعلومات أو البيانات"".....

(314) تنص هذه المادة " يعاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على سنتين وبغرامة لا تقل عن مائة ريال ولا تزيد على خمسمائة ريال أو بإحدى هاتين العقوبتين كل من استولى أو حصل على نحو غير مشروع على بيانات تخص الغير تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات""

(315) تنص هذه المادة "" تضاعف العقوبة ذا ارتكبت الأفعال المشار إليها في المادة (٢٧٦) مكرر و(٢٧٦) مكرر (١) من مستخدمي الكمبيوتر.

(316) تنص هذه المادة على "" إذا كان للفعل عدة اوصاف ، ذكرت جميعها في الحكم بدون أن يفرض على الفاعل سوى العقوبة التي يستلزمها الوصف الأشد"".......

الفصل الثالث

الإشكالات الإجرائية لجريمة الدخول غير المشروع عن قصد

بالرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الصّعد وفي شتّى ميادين الحياة المعاصرة[٣١٧] ، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في

(317) جميل عبدالباقي الصغير ، المرجع السابق، ص٤ ـ ٥ ؛ عبدالله العلوي البلغيثي : "الإجرام المعاصر ـ أسبابه وأساليب مواجهته" ، ورقة مقدمة ضمن أشغال المناظرة الوطنية حول (السياسة الجنائية بالمغرب : واقع وآفاق) ، التي نظمتها وزارة العدل بمكناس خلال الفترة من ٩ ـ ١١ دجنبر (ديسمبر) ٢٠٠٤ ، المجلد الأول ، (الأعمال التحضيرية) ، الطبعة الثانية ، منشورات جمعية نشر المعلومة القانونية والقضائية ، سلسلة الندوات والأيام الدراسية ، العدد (٣) ، ٢٠٠٤ ، ص٢٢٢.

المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة والانحراف عن الأغراض المتوخاة منها ، تبدّت في تفشي طائفة من الظواهر الإجرامية المستحدثة ، ألا وهي ظاهرة الجرائم المعلوماتية[٣١٨] .

وقد ازدادت هذه المخاطر تفاقماً في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات الدولية (الإنترنت) واسعة الانتشار ، ما أفرز نوعاً جديداً من الجرائم لم يكن معهوداً من قبل ممثلاً في الجرائم العابرة للحدود Transnational Crimes ، ولم يعد خطرها أو آثارها محصورة في النطاق الإقليمي لدولة بعينها ، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة (أجهزة العدالة الجنائية بجميع مستوياتها وعلى اختلاف أدوارها) [٣١٩]، وبالذات فيما يخص إثبات هذه الجرائم ، وآلية مباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة ؛ ذلك أن ملاحقة الجناة وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم في نطاق إقليم دولة أخرى ، وهو ما يصطدم بمبدأ السيادة الإقليمية للدول عملاً بمبدأ إقليمية القانون الجنائي ، الذي يفضي إلى تنازع الاختصاص القضائي بسبب صعوبة تحديد مكان وقوع الجريمة المعلوماتية عبر الوطنية .

ومن ثم كان لابدّ ـــ والأمر كذلك ـــ من البحث عن حلول مناسبة لهذه الإشكاليات تتوافق مع طبيعة هذه الجرائم المستحدثة فيما يخص قبول الدليل الرقمي ومباشرة بعض إجراءات التحقيق عبر الفضاء المعلوماتي وكذلك تحديد معايير الاختصاص[٣٢٠] .

المبحث الاول :الاختصاص القضائي لجريمة الدخول غير المشروع

إن قواعد القانون الجنائي (بشقّيه الموضوعي والإجرائي) تخضع في تطبيقها من حيث المكان لمبدأ مستقر ومعروف ، ألا وهو مبدأ الإقليمية ، الذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى

([318]) ذياب البداينة ، المنظور الاقتصادي والتقني والجريمة المنظمة ، ضمن أبحاث حلقة علمية حول الجريمة المنظمة وأساليب مكافحتها ، التي نظمتها أكاديمية نايف العربية للعلوم الأمنية ، ١٤ ـ ١٨ نوفمبر ١٩٩٨ ، مركز الدراسات والبحوث ـ الرياض ، ١٩٩٩ ، ص٢٠٩ وما بعدها ؛ موسى مسعود ارحومة ، ؛ الإرهاب والإنترنت ، بحث مقدم إلى المؤتمر الدولي لجامعة الحسين بن طلال بعنوان : الإرهاب في العصر الرقمي ، ص٨١ ، المنعقد بمدينة معان ـ الأردن ، خلال الفترة ١٠ ـ ٢٠٠٨/٧/١٣ ، ص١ وما يليها ؛ جميل الصغير ، المرجع السابق ، ص٥ وما بعدها .

([319]) عمر محمد بن يونس ، المرجع السابق ، ص٧٨٥ وما بعدها .

([320]) أسامة أحمد المناعسة ، جرائم الحاسب الآلي والإنترنت ـ دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر ـ عمان ـ الأردن ، ٢٠٠٠

الناشئة عنها ، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبـــي، وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقاً لحدودها المعترف بها في القانون الدولي إلاّ في أحوال استثنائية اقتضتها حماية المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام.

والأصل أن عناصر الركن المادي للجريمة تكتمل في مكان واحد ، أو بالأحرى في نطاق إقليم دولة واحدة ، حيث يقع السلوك الإجرامي (النشاط) ، وتترتب عليه آثاره الضارة في إقليم دولة واحدة ، كأن يقدم أحدهم على طعن المجني عليه أو إطلاق الرصاص عليه ، ما يفضي إلى وفاته في الحال أو بعد لحظة وجيزة ، ومن ثم تعتبر الجريمة مرتكبة في هذا المكان . وعلى ضوء ذلك يتحدد القانون الواجب التطبيق ، وبالتبعية المحكمة المختصة بنظر الدعوى .

بيد أن بعض الجرائم يتجاوز مداها ــ أحياناً ــ حدود الدولة ، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان بحيث يمكن وقوع السلوك في مكان ، وليكن إقليم دولة (س) ، في حين تتحقق النتيجة الجرميّة الضارة في نطاق إقليم دولة (ص) ، وهذا يقودنا إلى التساؤل عن مكان وقوع الجريمة في هذه الحالة، فهل هو مكان وقوع السلوك الإجرامي أم المكان الذي تحققت فيه النتيجة ؟

لقد حاول الفقه الإجابة عن ذلك منذ وقت مبكر ، من أجل حل مشكلة تنازع القوانين من حيث المكان (تنازع الاختصاص) بصدد هذه الفروض المثارة . وانقسم الرأي إلى ثلاثة اتجاهات[٣٢١]، فذهب الاتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه السلوك بقطع النظر عن المكان الذي تحققت فيه النتيجة ، أو من المفترض تحققها فيه ، وفي المقابل ذهب اتجاه آخر إلى أن مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة أو كان من المفترض تحققها فيه ، وبين هذا وذاك انبرى اتجاه ثالث إلى أن العبرة في ذلك تكون بمكان حصول أي منهما (السلوك أو النتيجة) ، ولكل مذهب من هذه المذاهب مبرراته وأسانيده التي تعززه وتدعمه[٣٢٢].

(321) موسى مسعود ارحومة ، تحديد النطاق المكاني لجرائم تلويث البيئة البحرية والقانون الواجب التطبيق ، ورقة مقدمة إلى المؤتمر العلمي الخامس لكلية الشريعة والقانون/جامعة إربد الأهلية بعنوان : "البيئة في ضوء الشريعة والقانون ـ واقع وتطلعات" ـ الأردن ، خلال الفترة ١٢ ـ ١٣/تموز (يوليو) ٢٠٠٦ ، ص٥ وما بعدها.

(322) موسى مسعود ارحومة ،الإشكاليــات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، ورقة عمل قدمت في المؤتمر المغاربي الاول حول المعلوماتية والقانون والذي عقد في أكاديمية الدراسات العليا ـ طرابلس خلال الفترة ٢٨ ـ ٢٩ / ١٠ / ٢٠٠٩

وبعيدا عن اختلافات الفقهاء حول مسألة الاختصاص في جرائم المعلوماتية عبر الحدود ، فقد حسم المشرع الأردني الاختصاص القضائي وما يمكن أن يثيره من إشكاليات ، عندما نص على ذلك في قانون جرائم أنظمة المعلومات / المادة 16- (يجوز إقامة دعوى الحق العام والحق الشخصي على المشتكى عليه أمام القضاء الأردني إذا ارتكبت أياً من الجرائم المنصوص عليها في هذا القانون باستخدام أنظمة معلومات داخل المملكة أو ألحقت أضرارا بأيٍ من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها ، كليا أو جزئيا ، أو ارتكبت من أحد الأشخاص المقيمين فيها) ، وسوف نتناول هذا المبحث في مطلبين: الأول يتحدث عن خصوصية جرائم الإنترنت والإشكالات التي يثيرها تنازع الاختصاص ، والثاني يتناول الاختصاص القضائي للمحاكم الأردنية.

المطلب الأول :خصوصية جرائم الإنترنت والإشكالات التي يثيرها تنازع الاختصاص

كما هو معلوم ، فإن الشبكة العنكبوتية لا تستأثر بها دولة بعينها ، ويتسنى لمستخدميها ولوجها من أية بقعة في العالم تقريباً من خلال جهاز حاسوب يكون متصلاً بها . فهي بطبيعتهاــ باعتبارها موزعة على أرجاء الكرة الأرضية ــ لا تحدّها حدود ، ومن ثم ــ والأمر كذلك ــ تكون من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة ، وهذا يستتبع ــ ولو نظرياً ــ عدم إمكان خضوعها لسلطان قانون جنائي معين .

وعملاً بمبدأ الإقليمية ، فإن كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها ، بصرف النظر عن جنسية مرتكب الجريمة ، الذي يحتمل معه تنازع القوانين حيال الواقعة الواحدة ، والذي يستتبع بالضرورة تنازع الاختصاص ، وبالذات فيما يتصل بالجرائم عبر الوطنية التي ترتكب عبر شبكة الإنترنت . فجريمة السبّ مثلاً عبر الرسائل الإلكترونية E. mails تقع أحياناً في بلد ويتلقاها الضحية في بلد آخر . وهنا ينبغي أن نشير إلى أن هذه الرسائل وغيرها من أدوات الاتصال عن بعد بواسطة هذه الشبكة تمر في كثير من الأحيان بأكثر من دولة قبل وصولها إلى بلد الاستقبال . ناهيك أن بعض الأفعال التي تُبث من خلال الإنترنت ، تعد أحياناً جريمة في بلد ومباحة في غيره من البلدان المرتبطة بهذه الشبكة .

ومن الأمثلة التي يسوقها الفقه على ذلك المراهنات على كرة القدم ، فهي غير مشروعة في بلد كفرنسا ، وجائزة في بلدان أخرى كما هو الحال في إنجلترا [٣٢٣].

وتطبيقاً للقواعد التي تحكم الاختصاص المكاني ، فإن جرائم الإنترنت العابرة للحدود Transnational Crimes تخضع في كثير من الأحيان لأكثر من قانون ، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة تحققت في نطاق بلد آخر ، فإن كلا البلدين يكون قانونه واجب التطبيق على الواقعة ، بمعنى أنه يتم تطبيق قانون كل دولة تحقق في نطاقها أحد عناصر الركن المادي للجريمة (السلوك أو النتيجة) ، فيكفي ليكون قانون البلد واجب التطبيق تلقي الضحية الرسالة الإلكترونية المجسدة لجريمة السبّ أو التهديد مثلاً في نطاقه ولو كان الفعل ذاته غير معاقب عليه في بلد المنشأ .

وبتطبيق ذلك على جريمة نسخ المصنفات ينعقد الاختصاص للدولة التي تم فعل النسخ على إقليمها ، باعتبار أن النسخ عن بعد يعد أحد العناصر المكونة لجريمة التقليد[٣٢٤].

وثمة أمر آخر يزيد الأمر تعقيداً وصعوبة في تحديد الاختصاص في جرائم الإنترنت عبر الوطنية بالذات ألا وهو تباين المعايير الوطنية فيما يتعلق بتحديد الاختصاص ، الأمر الذي يفضي عادة إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم .

فعلى سبيل المثال ، لو أن شخصاً ارتكب أياً من هذه الجرائم على إقليم دولة لا يحمل جنسيتها ، فقد يحدث التنازع بين قانون الدولة التي ارتُكِبت الجريمة على إقليمها وقانون الدولة التي ينتمي إليها .

أي أن الفعل يتنازعه قانونان ، قانون دولة الإقليم على أساس مبدأ الإقليمية ، وفي الوقت ذاته قد يخضع لقانون دولة الجاني عملاً بمبدأ الشخصية . ليس هذا فحسب ، بل قد ينعقد الاختصاص لدولة ثالثة متى كانت الجريمة ماسّة بمصالحها الحيوية وفقاً لمبدأ العينية[٣٢٥].

وحتى على فرض إمكانية إيجاد حل لهذه المشكلة من الزاوية القانونية ، فإنها تظل تصطدم بعقبات عملية بالنظر إلى الإجراءات المعقدة والطويلة التي يلزم اتباعها لمحاكمة الجاني الذي ارتكب أياً من هذه الجرائم ، وكانت إقامته خارج البلد الذي تتم فيها محاكمته ، والأمر

---

[323] جميل عبدالباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية-مصر، الطبعة ١، ص٤٣ ـ ٤٤.
[324] جميل عبد الباقي الصغير، المرجع السابق، صفحه ٤٩
[325] جميل عبد الباقي الصغير، المرجع السابق، ص٧٢ ـ ٧٣.

ينسحب أيضاً على تنفيذ الأحكام الصادرة بالخارج . ومن العوائق في ذلك مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد مرتين ، وكذلك عدم جواز تسليم الوطنيين .

وقد طُرحت مثل هذه المشاكل على القضاء المقارن، وتصدّى لها في أكثر من مناسبة. ففي القضاء الأمريكي، تشير التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء المذكور إلى جريمة وقعت في الخارج أن تكون آثارها قد مست مصالح أمريكية أو عرضتها للخطر ، تأسيساً على مبدأ الاختصاص الشخصي . من ذلك ما قضت به المحكمة العليا لولاية نيويورك بصدد جريمة انتهاك قانون المستهلك والدعاية الخادعة . والمبدأ ذاته كان قد طُبِّق في واقعة أخرى مؤداها قيام إحدى الشركات بولاية بنسلفانيا بالادعاء على أحد مزوّدي الإنترنت في ولاية كاليفورنيا بدعوى الاعتداء على علامة مسجلة في الولاية الأولى ، وقد أسست المحكمة حكمها على أن قضاء بنسلفانيا ينعقد له الاختصاص الشخصي على اعتبار أن مزود خدمة الإنترنت له مشتركون في الولاية ، بعبارة أخرى ، فإن القانون الأمريكي يتسع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية[٣٢٦].

وتكرس هذا الاتجاه القضائي فيما انتهت إليه الدائرة الخامسة الاستئنافية في قضية قمار ومراهنات عبر الإنترنت[٣٢٧]. وقد اعتبر القضاء المذكور مجرد وضع برمجية فك التشفير (PGP) على الإنترنت بمثابة تصدير لها ، وهو ما يخول المحاكم الأمريكية التصدي لها باعتبارها صاحبة الاختصاص، بصرف النظر عن مكان وضع البرمجية[٣٢٨].

كما تبنى القضاء الإنجليزي حلولاً مشابهة ، فهو يختص بنظر الدعاوى الناشئة عن إساءة استخدام الإنترنت ، متى كان ثمة ارتباط بين الواقعة المرتكبة وبريطانيا عملاً بقانون إساءة استخدام الحاسوب الصادر سنة ١٩٩٠ (The Computer Misuse Act of 1990) . فلكي ينعقد الاختصاص للمحاكم الإنجليزية ، يكفي امتداد آثار الواقعة إلى بريطانيا ، ولو كانت هذه الواقعة قد حدثت في الخارج ، وبصرف النظر عن محل إقامة الجاني . بعبارة أخرى ، يكفي أن يكون ناتج عمله أو أن نيته منصرفة إلى أن يكون ناتج عمله تعديلاً محظوراً في حاسوب موجود في بريطانيا[٣٢٩]. أما في فرنسا فيمتد اختصاص القضاء هناك إلى جرائم الإنترنت التي وقعت في

(326) عمر محمد بن يونس ، المرجع السابق ، ص٩٠٨
(327) عمر بن يونس ، المرجع السابق ، ص٩١٠
(328) عمر بن يونس ، المرجع السابق ، ص٩١٠
(329) عمر بن يونس ، المرجع السابق ، ص٩١١.

الخارج عملاً بقانون العقوبات الجديد متى كانت الظروف الواقعة تبرر مصلحة فرنسا في إعمال قانونها عليها(٣٣٠).

وصفوة القول ، إن جرائم الإنترنت عبر الوطنية ، لا تحدّها حدود خلافاً للجرائم التقليدية المعروفة ، الأمر الذي يجعلها في كثير من الأحيان تستعصي على الخضوع للقوالب القانونية التي تحكم مسألة الاختصاص المكاني . ومن ثم ، فإن الطبيعة الخاصة لهذا الصنف من الجرائم المستحدثة تتطلب تجاوز القوالب والمعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص ، والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها وآلية اقترافها والتخلص من آثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها .

وهذا بطبيعة الحال ، ينبغي ألاّ يُترك لمحض اجتهادات الفقه والقضاء ، وإنما يلزم تدخل المشرع لتحديد معايير الاختصاص التي يفترض عدم تضييق نطاقها ، بحيث يكون من الملائم أن ينعقد الاختصاص لقانون أي بلد أضرت به الجريمة أو من المتوقع أن تشكل خطورة على مصالحه الحيوية ، ولو كان مكان وقوعها خارج نطاق إقليمها . وبعض الفقه (٣٣١) ذهب إلى تبني مبدأ الاختصاص العالمي أو الشامل بهذا الخصوص من أجل تجنب الكثير من المشاكل الناجمة عن تحديد مكان وقوع الجريمة أو ترتب آثارها الضارة .

ونحن نؤيد هذا الاتجاه الفقهي الذي ذهب إلى ضرورة تبني مبدأ الاختصاص العالمي أو الشامل وذلك لسببين أولهما أن الجرائم الالكترونية تتشابه في وسائلها وأركانها عند معظم التشريعات الدولية والإقليمية وثانيهما ان مجال ارتكاب هذه الجرائم هو العالم الافتراضي وليس محصورا في بقعة جغرافية معينة .

---

(330) عمر بن يونس ، المرجع السابق ، ص٩١٢.

(331) موسى مسعود ارحومة ،الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، ورقة عمل قدمت في المؤتمر المغاربي الاول حول المعلوماتية والقانون والذي عقد في أكاديمية الدراسات العليا ـ طرابلس خلال الفترة ٢٨ ـ ٢٩ / ١٠ / ٢٠٠٩

المطلب الثاني : الاختصاص القضائي للمحاكم الأردنية

أشارت المادة (١٦)من قانون جرائم أنظمة المعلومات لعام ٢٠١٠[٣٣٢] إلى الاختصاص القضائي للمحاكم الأردنية متى تمت الجريمة باستخدام أنظمة معلومات داخل المملكة أو ألحقت إضرارا بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها أو ارتكبت من أحد الأشخاص المقيمين فيها، والغاية من وضع هذا النص هو منع اللجوء من قبل الفاعل إلى اختصاصات قضائية أخرى لارتكاب جريمة تستهدف مصالح داخل المملكة بغية التملص من العقاب، فقد يقرر أي شخص استخدام أنظمة معلومات أو مواقع الكترونية خارج المملكة لتنفيذ جرائم بحق مواطنيها أو المقيمين فيها كنوع من التحايل على القانون أو للإفلات من العقاب، وهذه المادة تحول دون ذلك[٣٣٣].

بتدقيق نصوص قانون العقوبات المادة ٧ منه المتعلقة بالصلاحية الإقليمية نجد انها حددت الاختصاص للمحاكم الأردنية اذا ارتكبت الجريمة داخل المملكة وعرفت داخل المملكة بأنه إذا تم على ارض هذه المملكة احد العناصر التي تؤلف الجريمة أو أي فعل من أفعال جريمة غير متجزئة أو فعل اشتراك أصلي أو فرعي[334].

وبقراءة نص المادة الخامسة من قانون أصول المحاكمات الجزائية الفقرة الرابعة منها نجد انها جاءت بقولها:

٥/٤-(يجوز إقامة دعوى الحق العام على المشتكي عليه أمام القضاء الأردني إذا ارتكبت الجريمة بوسائل الكترونية خارج المملكة وترتبت اثارها فيها ، كليا أو جزئيا ، أو على أي من مواطنيها[٣٣٥].

([332]) المادة ١٦- يجوز إقامة دعوى الحق العام والحق الشخصي على المشتكى عليه أمام القضاء الأردني إذا ارتكبت أياً من الجرائم المنصوص عليها في هذا القانون باستخدام أنظمة معلومات داخل المملكة أو الحقت اضراراً بأيٍ من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها ، كليا أو جزئيا ، او ارتكبت من أحد الأشخاص المقيمين فيها

([333])المذكرة الايضاحية لقانون جرائم أنظمة المعلومات http://www.slideshare.net/UrdunMubdi3/31-72010-2 18/11/2011

([334]) المحامي ياسر شقير ، تنازع القوانين والاختصاص القضائي وفق قانون جرائم أنظمة المعلومات المؤقت ، مقاله منشوره في جريدة الدستور الاردنية على الرابط:
http://www.addustour.com/ViewTopic.aspx?ac=\LocalAndGover\2010\12\LocalAndGover_issue1170_day28_id291621.htm#.Tukcj1bpiSo

([335])المادة الخامسة من قانون اصول المحاكمات الجزائية لعام ١٩٦١
http://www.lob.gov.jo/ui/laws/search_no.jsp?no=9&year=1961

ونجد أن نص المادة ١٦ مشابهه لما ورد في قانون الأصول ولا تغيير كبير في المفهوم أو السياسة التشريعية المحددة والمقررة للاختصاص وهو ان تكون احد اثار الجريمة قد وقعت في الأردن.

من خلال استقراء المواد القانونية السابقة نجد أن المشرع الأردني قد توسع في الاختصاص ليجد نفسه في مظلة ربما كانت أوسع مما قصده حيث إن طبيعة جرائم المعلومات أو التي ترتكب بطريق الانترنت عادة ما تتجاوز آثارها الحدود والأماكن الجغرافية ، ويدق تحديد الاختصاص هل هو لمكان وقوع الفعل أو الركن المادي أم احد عناصره ، أم لمكان الاستضافة أو مكان الاطلاع على نتائج هذا الفعل أو مكان ترتب آثاره والتي يمكن ان تكون في كافة دول العالم بما فيها الأردن ما يجعل القضاء الأردني هو المختص في تلك الجرائم على مستوى العالم.

بمقارنه هذا النص مع بعض النصوص المشابهة في القوانين الأخرى نجد مثلا أن قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧ ومحاولة منه للخروج من الدور العالمي في ملاحقة الجرائم أورد قيد على تطبيق القانون حيث اشترط للعقوبة شرطا اخر وهو ان يكون معاقبا عليها خارج السودان حيث جاء نص المادة الثانية بقولها (تطبق أحكام هذا القانون على أي من الجرائم المنصوص عليها فيـــه إذا ارتكبت كلياً أو جزئيا داخل أو خارج السودان أو امتد أثرها داخل السودان وسواء أكان الفاعل أصلياً أو شريكاً أو محرضاً على أن تكون تلك الجرائم معاقباً عليها خارج السودان مع مراعاة المبادئ العامة الواردة في القانون الجنائي لسنة ١٩٩١[336].

ونلاحظ أن شرط التجريم الخارجي الذي وضعه المشرع السوداني كان الهدف منه حتى لا يصطدم القضاء بقاعدة النظام العام الخارجي ومبدأ السيادة عند تطبيقه للنظام العام الداخلي.

وهذا الشرط له مبرراته فهو يجعل الجرائم التي تكون في نظر القانون المحلي أفعال مجرمة و نظر القانون الخارجي أفعال مباحة وغير معاقب عليها في الخارج ، وبالتالي ينزع الاختصاص من القضاء المحلي ويعفيه من التصدي لهذه الجرائم باعتبار ان إصدار الأحكام بها أصلا غير مجدي كون المجني عليه أو المدعي بالحق الشخصي لن يستطيع التنفيذ لا بالشق الجزائي ولا بالشق الحقوقي على الفاعل كونها أفعال مباحه في الخارج وتتعارض فكرة التجريم فيها مع النظام

([336]) المحامي ياسر شقير ، تنازع القوانين والاختصاص القضائي وفق قانون جرائم أنظمة المعلومات المؤقت ، مقاله منشوره في جريدة الدستور الاردنية على الرابط:
http://www.addustour.com/ViewTopic.aspx?ac=\LocalAndGover\2010\12\LocalAndGover_issue1170_day28_id291621.htm#.Tukcj1bpiSo ٢٠١١/١١/٢٢

العام في تلك الدول ، إلا انه بنفس الوقت يسقط الحق بالملاحقة لفعل يعتبر ارتكابه جريمة في نظر القانون ويؤثر على مبدأ السيادة.

تعتبر مشكلة تنازع القوانين هي المشكلة الأكبر في هذا القانون، فمثلا اذا وجد موقع اباحي ما في ولاية أو دولة أجنبية مما لا تجرم هذه الأفعال ومع ذلك يقوم بالترويج لتلك الإعمال على شبكة الانترنت وتم الدخول إلى هذا الموقع من الأردن من قبل قاصر وترتب ضرر له فما وضع الاختصاص القضائي الأردني.

نظرا لكون هذه الجرائم حديثه والقوانين التي تتداخل فيها عديدة نظرا لوقوع اثارها في غالب الأحيان في أكثر من دولة وتتنازع القوانين الخاصة بنظر الدعوى على ذلك الاختصاص ، مما يتثير مسالة تنازع الاختصاص القضائي في حال تصدت لها المحاكم الأردنية ، وهنا نتمنى على المشرع الأردني ان يضع معيارا أوضح للاختصاص سواء من حيث مكان وقوع الفعل أو مكان الاستضافة أو مكان الاطلاع على نتائج هذا الفعل أو مكان ترتب أثاره وقد تجتمع جميعها في احد هذه الجرائم في معظم دول العالم ويكون أثر هذه الجريمة في الأردن أثر ثانوي جدا لا يبرر جعل الاختصاص للمحاكم الأردنية فيستغل الآخرون هذا النص ويباشروا قضية جزائية في الأردن بين أطراف غير أردنيين بحجة ان أثرها قد تحقق في الأردن وتتنازع الدول في هذا الموضوع وتحاول كل دولة ونظرا لوجود عنصر أجنبي في هذه المعادلة أن تجعل الاختصاص لها.

المبحث الثاني :أساليب وإجراءات الضبط والإثبات والتحقيق في جريمة الدخول غير المشروع

إذا كانت ظاهرة الإجرام الإلكتروني أثارت العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجميع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم لكن النصوص التقليدية الواردة في قانون الإجراءات الجنائية تثير إشكالات كثيرة في حال تطبيقها على الجرائم المستحدثة ،ومن المشكلات الإجرائية التي يثيرها هذا النوع من الجرائم مدى إلتزام الشهود، أو المشتبه فيهم في كشف الرموز أو الأرقام أو كلمات السر المتعلقة بالبيانات أو البرامج ذات الصلة بالجريمة، كذلك يثور التساؤل عن مدى حجية المخرجات الإلكترونية في الإثبات، نظرا لطبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية(٣٣٧).

وتبدأ المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيا وكيانات منطقية غير مادية، وبالتالي يصعب من ناحية كشف هذه الجرائم، ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة الإجراءات في هذه المجال ، سرعة ودقة تنفيذ الجرائم الإلكترونية وإمكانية محو آثارها، وإخفاء الأدلة المتحصلة عنها عقب التنفيذ مباشرة، ويواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال، وقد يتعلقان ببيانات مخزنة في أنظمة أو شبكات إلكترونية موجودة بالخارج، ويثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق، مشكلات تتعلق بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات. وفي هذه الحالة يحتاج الأمر إلى تعاون دولي في مجالات البحث والتفتيش والتحقيق وجمع الأدلة، وتسليم المجرمين، بل وتنفيذ الأحكام الأجنبية الصادرة في هذا المجال. وسوف نتناول أساليب وإجراءات الضبط والإثبات والتحقيق في جريمة الدخول غير المشروع في مطلبين : المطلب الأول يبحث في إجراءات الضبط والتحقيق في جريمة الدخول غير المشروع والمطلب الثاني يبحث في إثبات الجرائم الإلكترونية باستخدام الوسائل الالكترونية.

([337]) خالد عبدالله القائفي ـ التحقيق الجنائي الرقمي، بحث منشور على الرابط التالي:
www.min-mag.com/researches/mindex.php ٢٠١١/١٠/٢٥

المطلب الأول : إجراءات الضبط والتحقيق في جريمة الدخول غير المشروع

نصت المادة ١٢- أ- على : (مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من الحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.

ب- مع مراعاة البند (أ) أعلاه من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة، و باستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج- للمحكمة المختصة الحكم بمصادرة الأجهزة و الأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة مرتكب الجريمة).[٣٣٨]

وباستقراء المادة (١٢) السالفة الذكر نجد انها أهم ما تعالجه هذه المادة هو التفتيش والضبط وكلاهما من المسائل المثيرة للجدل و يجب مراعاتهما بدقة حتى لا تنتهك الحريات الشخصية، ومما يجدر الإشارة اليه هو أن معظم التشريعات[٣٣٩] ومنها القانون النموذجي لجامعة الدول العربية أخذت بمبدأ التحفظ على خط سير البيانات وكذلك ضبط ومصادرة أجهزة الكمبيوتر في حال قيام الاعتقاد لديها بوجود المعلومات والبيانات داخلها وتركت لكل دولة عضو في الاتفاقية حق اتخاذ التدابير اللازمة لذلك وفق قوانينها الداخلية، بما في ذلك: ضبط وتأمين نظام المعلومات بما في ذلك أي جزء منه أو وسيط تخزين البيانات، عمل نسخة من البيانات والمعلومات،المحافظة

---

(338) قانــون جرائـــم أنظمـــة المعلومات لسنة ٢٠١٠ ، الجريدة الرسمية العدد(٥٠٥٦) بتاريخ ٢٠١٠/٩/١٦

(339) الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية لعام ٢٠٠١ http://eastlaws.blogspot.com/2010/03/23-11-2001.html ٢٠١١/١١/١٧

على تجانس بيانات الكمبيوتر ذات الصلة، جعل البيانات والمعلومات غير قابلة للوصول إليها أو الدخول إليها أو إزالتها من نظام المعلومات الذي يتم الدخول إليه. ولذلك تم النص في قانون جرائم أنظمة المعلومات على ضرورة مراعاة التشريعات ذات العلاقة ومن بينها قانون أصول المحاكمات الجزائية الذي ينظم التفتيش والضبط والذي يعرف الضابطة العدلية واختصاصاتها كما أن قانون الاتصالات يبين الأصول المتعلقة بتفتيش شركات الاتصالات المرخصة مما يتوجب مراعاته فيما تعلق بتلك الشركات وكذلك تراعى التشريعات الأخرى كل منها حسب نطاق تطبيقه، كما تم النص على ضرورة الحصول على إذن من المدعي العام المختص قبل الدخول إلى بيوت السكن وتفتيشها كون المدعي العام يستطيع تقدير وجود أسباب جدية تستدعي التفتيش، كما قصر اختصاص الضابطة العدلية على الضبط لمدة محددة ومن المعلوم أن الضبط لا يسمو إلى المصادرة التي هي من اختصاص المحكمة.

قد يلجأ بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج، فيصعب إثباتها، ويثور التساؤل حول حرية تدفق المعلومات وهل يصلح لتدفق البيانات الموجودة خارج الدولة المتعلقة بالجريمة محل البحث.

وسنعالج في هذا المطلب النقاط التالية :

الفرع الأول: التحري وكشف غموض الجريمة الإلكترونية.

الفرع الثاني : المعاينة.

الفرع الثالث : التفتيش.

الفرع الرابع : الضبط.

الفرع الخامس : مشكلات التفتيش والضبط.

الفرع الأول : في مجال التحري وكشف غموض جرائم الحاسب الآلي

الجرائم ذات الصلة بالحاسب الآلي، تتسم بحداثة أساليب ارتكابها، وسرعة تنفيذها، وسهولة إخفائها، وسرعة محو آثارها. هذه الخصائص العامة تقتضي ان تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها، وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها و ضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلا للجريمة.

وقد وجدت أجهزة الشرطة والتحقيق صعوبات جمة منذ ظهور هذا النوع المستحدث من الجرائم، سواء في كشف غموضها أو إجراء التفتيش والضبط اللازمين، أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية على نحو يمكنها من تحقيق المهمة المطلوبة منها وبالكفاءة المطلوبة ففي الفترة الأولى لظهور هذا النوع من الجرائم، وقعت الشرطة في أخطاء جسيمة أدت إلى الإضرار بالأجهزة أو الملفات، أو الأدلة الخاصة بإثبات الجريمة، ونعطي مثالا لهذا الخطأ من عمل الشرطة بالولايات المتحدة الأمريكية.

فقد حدث ان طلبت، إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، وقد حدث نتيجة لذلك ان تسببت دائرة البوليس بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج[٣٤٠].

وأساليب التحري أو التحقيق التقليدية، قد لا تصلح لكشف الجريمة، وضبط مرتكبيها، والتحفظ على أدلتها، ويمكن إجراء بعض التحريات المبدئية قبل عملية التفتيش أو الضبط والتحقيق، توصلا لكشف غموض الجريمة تمهيدا لضبط مرتكبها، وجميع الأدلة المتعلقة بها.

ويمكن للمجني عليه في هذه الجرائم التي يقدم خدمات كبيرة لرجال الشرطة، أو لسلطة التحقيق، فما يقدمه لرجل الشرطة من معلومات، تحقق فائدة كبيرة في معرفة طبيعة الجريمة التي وقعت وأساليب ارتكابها، والأدوات المستخدمة في ارتكابها، والأشخاص المشتبه فيهم، وبواعث الجريمة، وما إذا كان هناك شهود أم لا.

---

[340] هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة بأسيوط ،١٩٩٤ ، ص٢٩

الفرع الثاني: المعاينة

يقصد بالمعاينة مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها، أو محوها أو تعديلها[٣٤١].

والمعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، والأصل أن يحضر أطراف الدعوى المعاينة، وقد يقرر المحقق أن يجربها في غيبتهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور[٣٤٢]. ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه ان يبطلها.

وإذ تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها في الإثبات، فليس الحال كذلك بالنسبة للجرائم الإلكترونية، حيث ينذر أن يتخلف عن ارتكابها اثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الاثار الناجمة عنها إلى المحو أو التلف أو العبث بها[٣٤٣].

الفرع الثالث: التفتيش

التفتيش إجراء من إجراءات التحقيق، يهدف إلى البحث عن أشياء تتعلق بالجريمة، وكل ما يفيد بصفة عامة في كشف الحقيقة، سواء تعلق بالأشخاص أو بالأماكن.

وللتفتيش شروط موضوعية تتعلق :

أ- بسببه : وقوع جريمة بالفعل تعد جناية أو جنحة، وان يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه.

ب- الغاية منه : ضبط أشياء تفيد في كشف الحقيقة.

والشروط الشكلية تتحدد بــ:

أ- أن يكون الأمر بالتفتيش مسببا.

ب- حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش.

(341) محمد أبو العلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الالكترونية ، ورقة عمل قدمت في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان - ٢٨ نيسان ٢٠٠٣

(342) محمود نجيب حسني ، المرجع السابق ، ١٩٩٨، من ص ٥٢٨-٥٢٩

(343) هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة بأسيوط ،١٩٩٤ ، ص٥٩

ج- تحرير محضر بالتفتيش[٣٤٤].

ويثور السؤال عن إمكانية التفتيش وفقا للضوابط السابقة والغاية منه في مجال الجرائم الإلكترونية ؟ رغم أن البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي. ومع ذلك فيمكن ان يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالاسطوانات والأقراص الممغنطة، ومخرجات الحاسب.

فالتفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدِّلة المطلوبة وقد عرف المجلس الأوروبي هذا النوع من التفتيش بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الإلكتروني[٣٤٥].

ومحل التفتيش وما يتبعه من ضبط يشمل : البرامج أو الكيانات المنطقية Les logiciels، البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته ،والسجلات الخاصة بعمليات الدخول إلى نظام المعالجة الالية للبيانات، ويتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة[٣٤٦].

وبحسب الأصل يجب أن يصدر إذن التفتيش مكتوباً إلا أن هذا الشرط يحمل بعض المخاطر أحيانا وذلك في حالة ما إذا كان البحث عن أدلة الجريمة يستدعي أن يتم التفتيش في مكان آخر في نظام معلوماتي آخر غير الذي صدر بشأن الإذن المكتوب. والمخاطر تتمثل في إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها، خلال الفترة التي يراد الحصول على إذن مكتوب بشأنها. ولمواجهة هذه المخاطر، يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي اخر يوجد في اي مكان غير مكان البحث[٣٤٧].

ويثير إمتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الاخر مباشرة التفتيش لديه، ويرى البعض امتداد إذن التفتيش لا يكون إلا في حالتي هما التلبس، أو رضائه بالتفتيش[٣٤٨].

([344]) محمد أبو العلا عقيدة ، شرح قانون الاجراءات الجنائية ، ج١، ط١، ٢٠٠١، دار النهضة العربية ، ص ٤٣١

([345]) محمد أبو العلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الالكترونية ، ورقة عمل قدمت في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان - ٢٨ نيسان ٢٠٠٣

([346]) هشام رستم ،الجوانب الاجرائية للجرائم المعلوماتية ، المرجع السابق ، ص٧٧-٧٨

([347]) خالد عبدالله القائفي - التحقيق الجنائي الرقمي، بحث منشور على الرابط التالي: www.min-mag.com/researches/mindex.php ٢٠١١/١٠/٢٥

([348]) محمد أبو العلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الالكترونية ، ورقة عمل قدمت في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان - ٢٨ نيسان ٢٠٠٣

ويرى البعض أنه في حالة امتداد الإختصاص، فيمكن أن يصدر الأمر بالإمتداد شفويا من قاضي التحقيق، تحقيقا للسرعة المطلوبة، ثم يصدر فيما بعد الإذن المكتوب، وفي جميع الأحوال يجب أن يكون الإذن مسببا، لتتمكن الجهة القضائية من مراقبة مدى مشروعيته(٣٤٩).

والمشكلة الثانية التي تثور في حالة إمتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهاتها المختصة الإذن، ودخوله في المجال الجغرافي لدولة اخرى، حيث ينتهك الإمتداد سيادة الدولة الأخرى.

يرى جانب من الفقه أن هذا التفتيش الإلكتروني العابر للحدود لا يجوز في غياب اتفاقية دولية بين الدولتين تجيز هذا الإمتداد، أو على الأقل الحصول على إذن الدولة الأخرى. وهذا يؤكد أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني(٣٥٠).

ومع ذلك فقد أجازت المادة ٣٢ من الاتفاقية الأوروبية التي أعدها المجلس الأوروبي في صيغتها النهائية في ٢٥ مايو سنة ٢٠٠١ إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها، وذلك في حالتين(٣٥١) :

أ- إذا تعلق بمعلومات أو بيانات مباحة للجمهور.

ب- إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

الفرع الرابع : الضبط

الغاية من التفتيش ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، سواء أكان هذا الشيء أدوات استعملت في إرتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة.

ونظرا لكون الضبط محله في مجال الجرائم الإلكترونية، البيانات المعالجة إلكترونيا، فقد ثار التساؤل هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط ؟

حقيقة البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره(٣٥٢).

(349) محمد أبو العلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الالكترونية ، ورقة عمل قدمت في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان - ٢٨ نيسان ٢٠٠٣

(350) محمد أبو العلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الالكترونية ، ورقة عمل قدمت في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان - ٢٨ نيسان ٢٠٠٣

(351) محمد أبو العلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الالكترونية ، ورقة عمل قدمت في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان - ٢٨ نيسان ٢٠٠٣

وهذا السبب دعا المشرع في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلا عن الأشياء المادية المحسوسة، البيانات المعالجة إلكترونيا، أو إصدار تشريعات تتعلق بجرائم الحاسب الآلي، تتضمن القواعد الإجرائية المناسبة لهذه الصورة من البيانات،

وخشية من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش، فقد أعطت المادة ١٢ من قانون جرائم أنظمة المعلومات الحق في ضبط الأدلة الجرمية الالكترونية.

ويتم التحفظ على البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في إرتكابها، أو الآثار المتخلفة عنها وتفيد في كشف الحقيقة(٣٥٣).

مما تقدم يتضح لنا أن التحري والبحث والتحقيق وجميع الأدلة في مجال الجرائم الإلكترونية يكتنفُهُ الغموض، وتحيط به العديد من الصعاب، إلا انه لا مناص من مواصلة البحث والتحقيق وجمع الأدلة مع التطوير المستمر لوسائل البحث، ولأجهزة الشرطة وسلطات التحقيق، وتدعيم التعاون الدولي في هذا المجال.

الفرع الخامس :مشكلات التفتيش والضبط

تفتيش مسرح الجريمة وما يتصل به من أماكن وضبط المحرزات ذات العلاقة بالجرم أمور تنظمها القوانين، ويثور التساؤل حول مدى انطباق القواعد القائمة على حالة تفتيش نظم الكمبيوتر وقواعد البيانات.

أن تفتيش نظم الحواسيب تفتيش للفضاء الافتراضي ، وهو أمر يتعلق بالقدرة على تحديد المطلوب مسبقا، لان الخروج عن حدود امرالتفتيش قد يكون له عواقب قانونية أهمها بطلان الإجراءات لأنها خارج نطاق أمر التفتيش والضبط أو قد تنطوي الإجراءات على كشف خصوصية البيانات المخزنة في النظام.

ناهيك عن أن بوادرهذا الموضوع بدأت تظهر مع زيادة وتيرة النمو المتسارع الذى تشهده دول عربية عدة في استخدام النظم المعلوماتية فضلا عن ظروف السياسة الدولية والتبعية التكنولوجية وإدراكا لتجاوب الواقع الأردني مع ثورة تقنية المعلومات وما يشهده من جهود لتحويلها إلى عناصر تفيد في التنمية والتقدم، واستشرافا لمستقبل مسيرته صوب الأخذ في مختلف قطاعاته

---

(352) هشام رستم ،الجوانب الاجرائية للجرائم المعلوماتية ،المرجع السابق ، ص٦٨-٩٧

(353) محمد أبو العلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الالكترونية ، ورقة عمل قدمت في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان - ٢٨ نيسان ٢٠٠٣

بتقنية الحاسبات والمعلوماتية يغدو من الضروري الانكباب من الآن على تطوير وسائل الإثبات بما يواكب التطور في وسائل الإجرام المعلوماتي، فلقد ترتب على التطور المتزايد في استخدام الحاسب الآلي وما صاحبه من ظهور طائفة جديدة من الجرائم لم يكن لها وجود من قبل أن يصبح متطلبا من " السلطات القضائية " أن تتعامل مع أشكال مستحدثة من الأدلة في مجـــال الإثبات الجنائي.

جريمة الدخول غير المشروع كغيرها من الجرائم الالكترونية لها أركانها وعناصرها وتمر بذات المراحل التي تمر بها الجريمه كما في شأن الجرائم العادية كالسرقة والقتل وهذه المراحل هى التفكير في الجريمة والتحضير لها ثم تنفيذ الجريمة ومحاولة التخلص من آثارها.

ولذلك تثور هنا مسالة استخلاص الدليل الذي تثبت به الجريمة المعلوماتية،وإذا كان الاعتراف هو سيد الأدلة يليه شهادة الشهود فضلاً عن القرائن والآثار الناجمة عن النشاط الإجرامي بما لها من دور في إثبات الجريمة وكشف الحقائق فيها بالنسبة لجرائم قانون الجزاء التقليديه فإن قواعد هذا القانون تبدو قاصرة إزاء ملاحقة مرتكب الجريمة المعلوماتية مما حدا البعض(٣٥٤) على القول بأن قواعد قانون الجزاء التقليدية تواجه تحديات إزاء مواجهة الجريمة المعلوماتية وتبدو قاصرة عن مواجهة العديد من الأفعال التي تهدد مصالح إجتماعية واقتصادية ارتبطت بظهور وانتشار جهاز الحاسب الآلي وشبكة المعلومات الدولية(انترنت)، مما أدى إلى ظهور طائفة جديدة من الادله خاصه بالجريمه المعلوماتيه أطلق عليها الاداه التقنيه كالدليل الرقمي(digital evidence) .

هذا وحيث ان موضوع إثبات الجريمة المعلوماتية من الموضوعات التي تتميز بندرة التطبيق القضائي فانه تبرز للوجود مسألة صعوبة جمع الاستدلالات والأدلة في جريمة الدخول غير المشروع وفي كافة الجرائم الالكترونية إذ أن هذه النوعية من الجرائم توجد في بيئة لا تعتمد التعاملات فيها– أصلا– على الوثائق والمستندات المكتوبة بل على نبضات إليكترونية غير مرئية لا يمكن قراءتها بواسطة الحاسب والبيانات التي يمكن استخدامها كأدلة ضد الفاعل ويمكن في أقل من الثانية العبث بها أو محوها بالكامل لذلك فإن المصادفه وسوء الحظ لهما دور كبير في اكتشافها وذلك أكثر من الدور الذى تلعبه أساليب التدقيق والرقابة(٣٥٥) .

---

(354) راشد بن حمد البلوشي ورقه عمل حول الدليل في الجريمة المعلوماتية مقدمه الي المؤتمر الدولي الاول حول حماية امن المعلومات و الخصوصيه في قانون الانترنت" الفتره من ٢ الى ٤ يونيو ٢٠٠٨القاهرة جمهورية مصر العربية

(355) غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، مايو ٢٠٠٠.

لعل المبررات السابقة في شأن صعوبة استخلاص دليل الإثبات تحث بالتأكيد على ضرورة مسارعة رجال الاستدلال والتحقيق بتطوير وسائلهم البحثية وقدراتهم العلمية وليس بالضرورة أن يكون المحقق خبيراً في الحاسب الآلى ولكن لا بد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلى وحسن استغلالهم في كشف الجرائم وجمع الأدلة .

المطلب الثاني : إثبات جريمة الدخول غير المشروع باستخدام الوسائل الالكترونية

التطور الحالي الذي انعكس أثره على قانون العقوبات، قد انعكس أثره أيضا على قانون الإجراءات الجنائية، بحيث أن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الإلكترونية، كما وأن الإثبات الجنائي وهو أحد الموضوعات الهامة لهذا القانون قد تأثر بدوره بالتطور الهائل الذي لحق بالأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذي يتعين معه تغير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية.

ويرجع مدي صعوبة الإثبات في هذه الجرائم إلى عدة أسباب منها غياب الدليل المرئي :الجرائم التي تقع على العمليات الإلكترونية المختلفة كجرائم السرقة أو الاختلاس أو الاستيلاء أو الغش أو التزوير أو الإتلاف فإنه قد يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة..

فالجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإلكتروني تكون في منتهى الصعوبة لانها من النادر أن تخلف وراءها آثارا مرئية قد تكشف عنها أو يستدل من خلالها على الجناة.

ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه خاصة في حالات التلاعب في برامج الحاسبات.

لقد اتجهت النظم القانونية والقضائية والفقهية بوجه عام إلى قبول وسائل الإثبات التي توفر من حيث طبيعتها موثوقية في إثبات الواقعة وصلاحية للدليل محل الاحتجاج ، و بقراءة الاتجاه التشريعي العربي للتعامل مع تحديات الوسائل الالكترونية في الإثبات، فان البناء القانوني للتشريعات العربية عموما في حقل الإثبات لم يعرف الوسائل الالكترونية وتحديدا تلك التي لا

تنطوي على مخرجات مادية كالورق، وجاء مبناه قائما – بوجه عام مع عدد من الاستثناءات – على فكرة الكتابة ، المحرر، التوقيع، الصورة، التوثيق، التصديق، السجلات، المستندات، الأوراق ..... الخ ، وجميعها عناصر ذات مدلول مادي وان سعى البعض إلى توسيع مفهومها لتشمل الوسائل التقنية، وهي وان كان من الممكن شمولها الوسائل التقنية ذات المستخرجات التي تتوفر لها الحجية، فأنها لا تشمل الوسائل ذات المحتوى الالكتروني البحت وسنتناول في هذا المطلب :حجية المخرجات الالكترونية في الإثبات ، حجية المخرجات الالكترونية أمام القضاء الجزائي، الدليل الرقمي Digital Evidence ،الآثار المعلوماتية الرقمية ومسرح جريمة الكمبيوتر وخصصنا لكل محور فرعا مستقلا به.

الفرع الأول: حجية المخرجات الالكترونية في الإثبات

بداية يمكن القول أن نظم الإثبات في القانون المقارن تنقسم إلي مدرستين أساسيتين الأولى تتبع نظام الإثبات المعنوي أو المطلق وفيه لا يقيد المشرع أطرف الرابطة الإجرائية بتقديم أدلة معينة بل للقاضي أن يقتنع بأي دليل وهذا هو النظام السائد في القانون الفرنسي.

اما المدرسه الثانيه فتتبع نظام الإثبات القانوني أو المقيد وفيه يحدد القانون الأدلة التي يجوز تحقيقها والإستناد إليها في الحكم وهذا هو النظام السائد في القانون الإنجليزي.

و رغم إختلاف نظام المدرستين في نظام الإثبات إلا أن هناك ضوابط معينة تحكم الأدلة الناتجة عن الحاسب الآلي بشكل عام يلتزم بها القضاء لتحاشي سوء التصرف ولدعم وحماية حقوق الأطراف أو غيرها من الحقوق محل الإحترام وهذه الضوابط مدارها أصل البراءة و ما يتفرع عنه من نتائج وآثار وما يستتبعه من وجوب توافر شروط معينة في المخرجات الالكترونية حني يمكن الحكم بالإدانة ذلك أنه لا محل لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل إقتناع القاضي إلي حد الجزم واليقين فاذا كان القاضي لم ينته إلى أن المخرجات الالكترونية تصل بنسبة الفعل أو الجريمة المعلوماتية إلى المتهم المعلوماتي كان عليه أن يقضي بالبراءة...

عليه و تحقيقا لليقينية والشفوية والمشروعية في الدليل فان مجمل شروط قبول المخرجات الالكترونية تتلخص في المبادئ الثلاثه التاليه:

١.مبدأ يقينيه المخرجات الالكترونية.

٢.مبدأ وجوب مناقشة المخرجات الالكترونية

٣.مبدأ مشروعية المخرجات الالكترونية.

أولا: مبدأ يقينية المخرجات الالكترونية

اليقين القانوني يعني : تلك الحالة الناجمة عن القيمة التي يضفيها القانون على الأدلة ويفرضها على القاضي بمقتضى ما يصدره من قانونية محددة،فهو نوع من اليقين يتلقاه القاضي عن إرادة المشرع وهذا النوع من اليقين هو السائد في القانون الإنجليزي(٣٥٦)

إلا إن القانون العام في انجلترا لم يعد يأخذ بنظرية الأدلة القانونية على الإطلاق بل بدأ يتقبل مبدأ حرية تقدير الأدلة للقاضي لذلك فقد أصبح الحديث عن الإدانه بدون أي شك معقول أو الإدانه الخالية من أي شك هو السائد في القانون الإنجليزي حالياً.

ومن هذا المنطلق نجد أن القضاء الإنجليزي يملك حرية الحكم بالإدانة بناء على شهادة شخص واحد طالما أن هذه الشهادة تحقق اليقين(٣٥٧).

وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات كمبيوترية وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه.

ثانيا: مبدأ وجوب مناقشة المخرجات الالكترونية

ومفهوم مبدأ وجوب مناقشة المخرجات الالكترونية يعني بصفة عامة أن القاضي لا يمكن أن يؤسس إقتناعة إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، ولا يختلف الأمر بالنسبة للمخرجات الالكترونية بوصفها أدلة إثبات إذ ينبغي أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة الأطراف(٣٥٨).

وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى أو التحقيق الإبتدائي لكن بصفة مباشرة أمام القاضي ،وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الآلية ،وأيضاً بالنسبة لشهود الجرائم المعلوماتية الذين يكون قد سبق أن سمعت شهادتهم في التحقيق الإبتدائي فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة(٣٥٩) .

---

(356) نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي دراسة نظرية تطبيقية، منشورات الحلبي، بيروت، ط١، ٢٠٠٥ ، صفحه ٨٢
(357) هلالي عبد اللاه أحمد ، إلتزام الشاهد والإعلام في الجرائم المعلوماتية ، دراسة مقارنة ، القاهرة: دار النهضة العربية ، ١٩٩٧. صفحة٩١-٩٥
(358) هلالي عبد اللاه أحمد ، مرجع سابق ، ص ص ١٠٢-١٠٣
(359) محمد فهمي طلبة ، فيروسات ا لحاسب وأمن البيانات ، القاهرة ، مطابع الكتاب المصري الحديث سنة ، ١٩٩٢، ص ١٩ وما بعدها.

إن قاعدة وجوب مناقشة الدليل الجزائي سواء كان دليلاً تقليدياً أم كان ناتجاً عن الحاسب الآلي تعتبر ضمانات هامة وأكيدة للعدالة حتي لا يحكم القاضي الجزائي في الجرائم المعلوماتية بمعلوماته الشخصية أو بناء على رأي الغير[٣٦٠] .

وهذا ما أكدت عليه المحكمه العليا في سلطنة عمان في حكمها الصادر بجلسة ٢٠٠٢/١٠/٢٩م- الطعن رقم ٢٠٠٢/٧٢م حيث جاء في حكمها" أن تقدير الدليل بالصورة التي تكشف قناعة المحكمة من إطلاقات محكمة الموضوع لا تجوز إثارته أمام المحكمة العليا"[361].

ثالثا: مبدأ مشروعية المخرجات الالكترونية

ومبدأ مشروعية الدليل في الجرائم المعلوماتية يعني ان يكون هذا الدليل و ما يتضمنه قد تم وفق الإجراءت والقواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر أي أن مشروعية الدليل لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع بل يجب أيضاً مراعاة إعلانات حقوق الإنسان والمواثيق والإتفاقات الدولية وقواعد النظام العام وحسن الآداب السائدة في المجتمع بالإضافة إلي المبادئ التي استقرت عليها المحاكم العليا[٣٦٢].

ولذا يشير أحد الفقهاء الفرنسيين إلي أن القضاء قد قبل إستخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم الا انه اكد على أن يتم الحصول على الأدلة الجنائية ومن بينها المخرجات الالكترونية بطريقة شرعية ونزيهة[٣٦٣]

الفرع الثاني: حجية المخرجات الالكترونية أمام القضاء الجزائي

للقاضي سلطة تقديرية واسعة في تقدير الدليل ولكنها ليست سلطة مطلقة ،فالمشرع وضع القيود من حيث القواعد التي تحدد كيفية حصوله عليه والشروط التي يتعين عليه تطلبها فيه ومخالفة هذه الشروط قد تهدر قيمة الدليل وتشوب قضاءه بالبطلان[٣٦٤].

أن مشكلة حجية المخرجات الالكترونية على المستوي الجزائي لا تبدو ملحة أو عاجلة في نظر الفقهاء الفرنسيين فالأساس هو حرية الأدلة وحرية القاضي في تقدير هذه الأدلة. والواقع أن الفقة الفرنسي يدرس حجية المخرجات الالكترونية في المواد الجنائية ضمن مسألة قبول الأدلة الناشئة

---

(360) راشد بن حمد البلوشي ، ورقه عمل حول الدليل في الجريمة المعلوماتية مقدمه الي المؤتمر الدولي الاول حول "حماية امن المعلومات و الخصوصيه في قانونالانترنت" الفتره من ٢ الى ٤ يونيو ٢٠٠٨ القاهرة جمهورية مصر العربية

(361) راشد بن حمد البلوشي ، ورقه عمل حول الدليل في الجريمة المعلوماتية مقدمه الي المؤتمر الدولي الاول حول "حماية امن المعلومات و الخصوصيه في قانونالانترنت" الفتره من ٢ الى ٤ يونيو ٢٠٠٨ القاهرة جمهورية مصر العربية

(362) احمد ضياء الدين محمد خليل ، مشروعية الدليل في المواد الجنائية ، كلية الحقوق ، جامعة عين شمس سنة ١٩٨٢ ، محمد سامي الملا ، اعتراف المتهم ، رسالة دكتوراه ، جامعة القاهرة سنة ١٩٦٩ ص ٢٤ وما بعدها.

(363) هلالي عبد اللاه أحمد ،مرجع سابق ،ص ١٢١ .

(364) هلالي عبد اللاه أحمد ، مرجع سابق ، ص ٣٠

عن الآلة أو الأدلة العلمية مثل الرادارات والأجهزة السينمائية وأجهزة التصوير وأشرطه التسجيل وأجهزة التصنت.

وعلى هذا الأساس حكمت محكمة النقض الفرنسية أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي[٣٦٥].

اما فيما يتعلق بالتطبيقات الخاصة بالأدلة الناتجة عن الحاسبات الآلية في بريطانيا ، وفي قضية جولد وشفرين سنة ١٩٨٨ حاول الدفاع ان يشكك في أدلة الإثبات . مدعياً أن الكثير من الأدلة التي بني عليها الإدعاء إتهامة يجب إستبعادها حسب تقدير القاضي وفقاً للقسم ٧٨ من قانون البوليس والأثبات الجزائي لسنة ١٩٨٤ كما انتقد أساليب التحري في النظام البريطاني للأجهزة التليفونية لإثبات الوصول غير المصرح به للجاني في بيرستل وخاصة استخدام جهاز رصد البيانات وجهاز رصد المكالمات (ميراكل المعجزة) والذي حدد هوية إثنين من المتهمين اللذين تمت اعتراض اتصالاتهما بل لقد ادعى الدفاع ان هيئة التليفونات البريطانية قد ارتكبت جريمة عند قيامها بجمع الأدلة ، هذه الادعاءات رفضها القاضي بتلر الذي كان ينظر للقضية وبالتالي لم ينجح الاستئناف في حين أن القسم ٧٨ لا يمس مباشرة أنشطة الشرطة في التصنت إلا أن هذا القسم كما يتم تفسيره حالياً قادر على استبعاد أي دليل يتم الحصول عليه عن طريق شرك.

لكن ما مدى تمسك القانون الإنجليزي بنظرية ثمار الشجرة المسمومة[٣٦٦] في مجال المخرجات الالكترونية ؟جوهر هذه النظرية : أنه أذا كانت الشجرة السامة لا تطرح إلا ثمار سامة لآن الطبيعة السامة من الأصل لابد أن تنتقل بالضرورة إلي الفرع فأن نفس الشئ يحدث بالنسبة للدليل الجزائي في عدم مشروعية الدليل الأصلي تمتد إلي الدليل الفرعي أو الدليل اللاحق وبالتالي يتعين استبعادهما معاً طالما أن الدليل الثاني يرتبط بالأول ويترتب عليه[٣٦٧]

ومن هذا المنطلق تنص الفقرة الرابعة من المادة ٧٦ من قانون البوليس والإثبات الجزائي سالف الذكر على أنه أذا كان الاعتراف غير مقبول فإن كل ما يترتب عليه بعد ذلك يصبح غير مقبول يستوي في ذلك الأدلة التقليدية أو الأدلة الناتجة عن الحاسب الآلي[٣٦٨]

([365]) هلالي عبد ا للاه أحمد،مرجع سابق ص ٣٠-٤٢. كذلك د. أحمد عوض بلال ، التطبيقات المعاصرة للنظام الإتهامي في القانون الأنجلو أمريكي ، القاهرة ، دار النهضة العربية ،سنة ١٩٩٢-١٩٩٣ ، ص ٢٦١-٢٦٧.

([366])هو في الأصل اصطلاح ظهر في أمريكا ثم انتقل إلي إنجلترا.

([367]) ويقابل هذه النظرية في الشريعة الإسلامية القاعدة الأصولية أنه لا يبني صحيح على باطل أو ما بنى على باطل فهو باطل

([368]) هلالي عبد اللاه أحمد ، المرجع السابق، ص ١٣٥

الفرع الثالث: الدليل الرقمي Digital Evidence

الدليل الرقمي:هو الدليل المأخوذ من أجهزة الكمبيوتر، وهو يكون في شكل مجالات مغناطيسية أو نبضات كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء.

ويمتاز الدليل الرقمي عن الدليل المادي المأخوذ من مسرح الجريمة المعتاد، بما يلي[٣٦٩]:

١.طريقة نسخ الدليل الرقمي من أجهزة الكمبيوتر تقلل أو تعدم تقريباً مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء.

٢.باستخدام التطبيقات والبرامج الصحيحة، يكون من السهولة تحديد ما إذا كان الدليل الرقمي، قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل.

٣.الصعوبة النسبية لتحطيم أو محو الدليل، حتى في حالة إصدار أمر من قبل الجاني بإزالته من أجهزة الكمبيوتر، فيمكن للدليل الرقمي أن يعاد تظهيره من خلال الكمبيوتر دسك.

٤.نشاط الجاني لمحو الدليل، يسجل كدليل أيضاً، حيث أن نسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقاً لاستخدامها كدليل إدانة ضده.

٥.الاتساع العالمي لمسرح الدليل الرقمي، يُمَكّن مستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية، وبمناطق مختلفة من العالم، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبياً.

6.امتيازه بالسعة التخزينية العالمية، فآلة الفيديو الرقمية، يُمكنها تخزين مئات الصور، ودسك صغير يمكنه تخزين مكتبة صغيرة وهكذا.

٧.يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت فالدليل الرقمي يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

وعادة ما توجد الأدلة الرقمية في مخرجات الطابعة والتقارير والرسوم وفي أجهزة الكمبيوتر وملحقاتها وفي الأقراص المرنة والصلبة وأشرطة تخزين المعلومات وفي أجهزة المودم والبرامج

---

(369) راشد بن حمد البلوشي ورقه عمل حول الدليل في الجريمة المعلوماتية مقدمه الي المؤتمر الدولي الاول حول حماية امن المعلومات و الخصوصيه في قانون الانترنت" الفتره من ٢ الى ٤ يونيو ٢٠٠٨القاهرة جمهورية مصر العربية

وأجهزة التصوير ومواقع الويب والبريد الإلكتروني ولذلك تستخدم عدة طرق أو أدوات تساهم في جمع الأدلة الرقمية منها:

.أولا: برنامج أذن التفتيشComputer Search Warrant Program

وهو برنامج قاعدة بيانات، يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

ثانيا: قرص بدء تشغيل الكمبيوتر:(Bootable Diskette([370]

وهو قرص يُمكن المحقق من تشغيل الكمبيوتر، إذا كان نظام التشغيل فيه محمياً بكلمة مرور ويجب أن يكون القرص مزوداً ببرنامج مضاعفة المساحة Double space فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

ثالثا:برنامج معالجة الملفات مثلX tree Pro Gold

وهو برنامج يُمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يُمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها[٣٧١].

رابعا: برنامج النسخ مثلLap Link

وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي Parallel Port أو على التوالي Serial Port وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

خامسا:برامج كشف الدسك مثلAMA Disk, View disk

ويمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة)[٣٧٢].

([370]) تقنيات الأدلة الجنائية الإلكترونية ن مقال علمي للكاتبة جمانة كاظم علي الخليفة ، منشرو على الانترنت : http://coeia.edu.sa/images/stories/PDFs/techniques-of-e-forensic.pdf ٢٠١١/١٢/٣

([371]) تقنيات الأدلة الجنائية الإلكترونية ن مقال علمي للكاتبة جمانة كاظم علي الخليفة ، منشرو على الانترنت : http://coeia.edu.sa/images/stories/PDFs/techniques-of-e-forensic.pdf ٢٠١١/١٢/٣

([372]) تقنيات الأدلة الجنائية الإلكترونية ن مقال علمي للكاتبة جمانة كاظم علي الخليفة ، منشرو على الانترنت : http://coeia.edu.sa/images/stories/PDFs/techniques-of-e-forensic.pdf ٢٠١١/١٢/٣

سادسا :برامج اتصالات مثلLANtastic

وهو يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب. هذه هي أهم الطرق العامة لجمع الأدلة الرقمية، والتي يجب أن يقوم بها خبراء في هذا المجال نظراً لعلمية ودقة هذه الأدلة.

ويوجد برنامج يسمى Trace route يمكنه تقديم قائمة بالطرق والمسالك التي يمكن أن تسلكها الحزم المعلوماتية للوصول إلى الكمبيوتر المقصود، وعادة ما يتم إدراج هذا البرنامج ضمن نظم التشغيل الرئيسة Operating System وعادة تسلك المعلومات أو الحزم المعلوماتية نفس المسار دائماً، ما لم يتم تغيير هذا الاتجاه بتغير الأجهزة مثلاً.( )

ويعتبر هذا البرنامج برنامج Trace route ذا أهمية في الكشف الجنائي، حيث أنه يحدد بدقة أي من أجهزة الكمبيوترات التي اشتركت في نقل البيانات على الإنترنت، وتحديد مساراتها حتى وصلت إلى المرسل إليه وتحديد الملفات التي تم الولوج إليها لذلك تصبح كل المسارات بها آثار أو أدلة رقمية يمكن الاستدلال بها على نشاط الجاني، كما أنه من جهة أخرى يحدد المسار الذي أخذته المعلومة وتحديد أي اختراق أو عبور أو تجاوز خلال الإعداد للجريمة، كما أنه يستدعي أو يمكنه أن يحيط بكافة المعلومات المتعلقة بدخول أشخاص مواقع معينة وتحديد مسارات ولوجهم وخروجهم من المواقع المحددة.

الفرع الرابع :الآثار المعلوماتية الرقمية ومسرح جريمة الكمبيوتر

وهي الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية.[373]

ويلاحظ أن هذه الآثار تكون في شكل رئيس هو الشكل الرقمي، لأن البيانات داخل الكمبيوتر سواء أكانت في شكل نصوص أم أحرف أم أرقام أم أصوات أم صور أم فيديو تتحول إلى صيغة رقمية، حيث ترتكز تكنولوجيا المعلوماتية الحديثة على تقنية الترقيم التي تعني ترجمة أو تحويل

(373) خالد ممدوح ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، ٢٠٠٩ ، ط١، صفحه ٢٧ وما بعدها

أي مستند معلوماتي مؤلف من نصوص أو صور أو أصوات أو بيانات إلى نظام ثنائي في تمثيل الأعداد يفهمه الكمبيوتر قوامه الرقمان(0و1)[٣٧٤].

وتمتاز النصوص الرقمية بسهولة استنساخها بوقت قصير وبكلفة هامشية دون المساس بالأصل ولا بنوعية النسخ، فالنسخ تكرار للأصل وليس نسخة منه، وتمتاز أيضاً البيانات الرقمية بسهولة التلاعب بها سواء تعديلاً أو إتلافاً أو إدراجاً في مستندات أو بيانات رقمية أخرى وبسرعة متناهية.

ويلاحظ أن الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الكمبيوتر من الممكن أن تكون ثرية جداً فيما تحتويه من معلومات مثل صفحات المواقع المختلفة Web Pages والبريد الإلكترونيEmail ، الفيديو الرقميdigital Video وغيرها ، لذلك فإن الآثار الرقمية تشمل رؤية لمسرح الجريمة الحقيقي، ومسرح الجريمة الرقمي نفسه فإذا كانت هناك جريمة حدثت فعلياً في العالم الحقيقي واستخدام كمبيوتر بطريقة ما في أحد أفعالها فإن رجال الشرطة أو مقتفو الأثر الجنائي يجب عليهم أن يبحثوا في كل من المَسّرَحَينْ المسرح الحقيقي والمسرح المعلوماتي الرقمي.

ملفات الولوج وجداول الحالة التشغيلية يمكن أن تحتوي على معلومات عن مصادر وطبيعة الجريمة محل التحقيق أو البحث، حيث تحتوي ملفات الولوج على عناوين IP للكمبيوتر المستخدم والكمبيوتر الوسيط أو الرئيس أو الخادم، وتحتوي على معلومات من كافة الأنشطة التي قام بها المستخدم أو حاول أن يقوم بها عند استخدامه للشبكة المعلوماتية وتحتوي كذلك على معلومات بشأن أنواع الاتصالات التي تمت وكل هذه المعلومات ممكن أن تستخدم في تصنيف وتخصيص وتوثيق الدليل الرقمي تجاه الجريمة محل البحث والتحقيق.

وحاليا يمكن القول ان فرق التحقيق الجنائي المختصة بالكشف عن الأدلة الرقمية تستخدم وسائل حديثة وعديدة في هذا المجال منها[٣٧٥] :

([374]) علي محمود علي حموده ، الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي لمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ر:اكادمية شرطة دبي ، مركز البحوث والدراسات رقم العدد : ١ السنة : ٢٠٠٣تاريخ الإنعقاد: ٢٦ نيسان ٢٠٠٣تاريخ الإنتهاء: ٢٨ نيسان ٢٠٠٣

([375]) " جرائم الحاسوب"، ورقة مقدمة من قبل النقيب المهندس رائد بلاسمه الى مؤتمر الامن والسلامة المعلوماتية الذي عقد في الجامعه الاردنية في الفترة من ٢١-٢٠١١/١١/٢٣

١.محطات لفحص الأدلة الرقمية وتحليلها من خلال استخدام نظام Encase[376]و FTK[377]وحسب ماهو معمول به في اكثر دول العالم تقدماً.

٢. نظام الRainbow الخاص بفك تشفير كلمات السر والحماية بما فيها الكلمات المعقدة.

(376) هذا البرنامج تستخدمه الجهات الامنية من مخابرات وشرطة (مباحث) للبحث والتنقيب داخل اجهزة الكمبيوتر الخاصة بالاشخاص المشتبه بهم ومن ثم توثيق اية ادلة وبراهين وتقديمها في المحاكم ضد المتهمين.

(377) هذا البرنامج يقوم بأخذ نسخه من الهاردسك او الفلاش مميري و CD و DVD واي ماده تخزينية كما يقوم بكسر كلمات السر المخزنة على الاجهزة

الخاتمة

تعد هذه الدراسة حصيلة جهد متواضع قمنا به بهدف التصدي لهذا الموضوع ذو الصبغة العلمية الغريبة، والتي في رأينا غريبة على رجال القانون، لكن لا يجب أن يكون هذا الطابع العلمي حائلا دون توسيع قاعدة النقاش حول الإجرام المعلوماتي، وحتى لا يبقى موضوع الجريمة المعلوماتية من المناطق المحرمة التي يتجنب معظم الباحثين ودارسي القانون الخوض فيها.

لا ننكر الصعوبة التي واجهتنا لإنجاز هذا البحث نظرا لنقص الدراسات في هذا الميدان حتى نتمكن من الإحاطة بالجوانب القانونية كاملة لجريمة الدخول غير المشروع حسب نصوص قانون جرائم أنظمة المعلومات لعام ٢٠١٠ ، إلا أن ذلك لا يمنع من أننا توصلنا في ختام هذه الدراسة إلى عدة نتائج يمكن بلورتها فيما يلي:

النتائج

١- ثورة التكنولوجيا وانتشار الحاسب الآلي أديا إلى تغيير في المفاهيم التقليدية للجريمة سواءً من حيث وسائل ارتكابها ، أو طبيعة الدليل وطرق انتشاله ، بالإضافة إلى مدى الحجية في الإثبات.

٢- تعتبر جريمة الدخول غير المشروع لنظام المعلومات جريمة ذات طابع تقني وحسنا فعل المشرع الأردني بإيجاد حماية قانونية لها بنص المادة الثالثة من قانون جرائم أنظمة المعلومات .

٣- تتميز جريمة الدخول غير المشروع لنظام المعلومات جريمة تعتمد على الذكاء والمهارة التقنية دون أدنى مجهود عضلي.

٤- الشق المعنوي للحاسب الآلي (البرامج ، والبيانات ، والمعلومات) أصبحت محمية بنصوص المواد في قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ .

٥- نقص المعرفة العلمية ، والتقنية ، والخبرة في مجال الحاسب الآلي والجرائم المرتبطة به ، سواءً من جهة التحقيق أو القضاء أو الفقه .

٦- أحسن المشرع الأردني صنعا عندما جرّم محاولة الإخلال بسير نظام المعلومات أو المواقع الالكترونية إذا كانت نتيجتها سوف تؤدي مسح أو إتلاف أو تعديل البيانات المبرمجة .

٧- أحسن المشرع الأردني صنعا عندما عاقب على الدخول غير المشروع لنظم المعلومات واعتباره الدخول المجرد غير المشروع جريمة كاملة ، دون حاجة إلى تحقق نتيجة ضارة لما لأهمية البيانات والمعلومات الموجود داخل نظم الحاسبات والمواقع الالكترونية

التوصيات:

١. من الضروري توفير حماية أمنية للنظام المعلوماتي للتصدي لمحاولة المقتحمين للنظام المعلوماتي وذلك على مستويين أولهما برامج حماية متطورة للنظام المعلوماتي وثانيهما تحصين المؤسسات التجارية والحكومية وغيرها بتوفير أنظمة ذكية لابواب الغرف التي يوجد فيها مواقع الخوادم (servers) بحيث يتم الدخول اليها بالبطاقات الذكية ومن قبل المخوليين فقط.

٢. نتمنى على المشرع الأردني تجريم إتلاف البيانات أو العبث فيها بنص خاص دون اشتراط أن يكون الدخول غير مشروع وقصدا ، فقد يكون الدخول لنظام المعلومات مشروعا ويتم إتلاف البيانات من قبل الجاني ، ففي هذه الحالة فلا مسؤولية عليه وفق القانون الحالي ولا بد من إدخال نص قانوني جديد يعالج هذه الثغرة.

٣. من الضروري إيجاد نصوص قانونية تبين مسئولية مزودي الخدمات ، فالنصوص الموجودة في قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ لا تتضمن تحديد لمسؤولية مزودي الخدمات.

٤. نتمنى على المشرع الأردني إدخال نصوص قانونية لقانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ من اجل تقرير مسؤولية للشخص المعنوي كالشركات وغيرها في حال ارتكاب أحد افرادها جريمة الكترونية .

٥.من الضروري ايجاد نص في قانون جرائم أنظمة المعلومات المؤقت لعام ٢٠١٠ يقرر العقاب على الشروع في الجريمة.

6.نتمنى على المشرع الأردني رفع الحد الأدنى والأعلى للعقوبة في حال ارتكاب جريمة الدخول غير المشروع إلى نظام المعلومات بهدف إتلافها أو تعديلها أو بهدف إلغاء موقع الكتروني أسوة بالتشريعات المقارنة .

7. نرى أن تسمية قانون جرائم أنظمة المعلومات لعام ٢٠١٠ جانبها الصواب ، وكان الأفضل بالمشرع الأردني تسمية هذا القانون بقانون مكافحة جرائم أنظمة المعلومات لعام٢٠١٠ ، فنصوص القانون شرّعت لمكافحة جرائم المعلوماتية وليس النص على هذه الجرائم.

المراجـــــــــــــع

أولا:الكتب

احمد ، هلالي (١٩٩٧) ، **إلتزام الشاهد والإعلام في الجرائم المعلوماتية / دراسة مقارنة** ، ط(١) ،القاهره: دار النهضة العربية للنشر والتوزيع .

احمد ، هلالي (٢٠٠٣) ، **الجوانب الموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست** الموقعه في ٢٠٠١/١١/٢٣ ، طبعة (١)، القاهره : دار النهضة العربية للنشر والتوزيع .

البقمي ، ناصر (٢٠٠٩)- **مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية** ، ط(١) ، دبي : مركز الإمارات للدراسات والبحوث الاستراتيجية.

الحسيني ، عمر(١٩٩٥) ، **المشكلات الهامة في الجرائم المتصلة بالحاسب الالي وابعادها الدولية** ، ط(١) ، القاهره : دار النهضة.

الخلف ، علي و الشاوي ، سلطان (١٩٨٢) ، **الاحكام العامة في قانون العقوبات** ، بدون طبعة ، الكويت : دار الرسالة -الكويت .

السعيد ، كامل (١٩٨٣) ، **شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن**، ط(٢)عمان : دار الفكر للنشر والتوزيع ،

الشوا ، محمد (١٩٩٨) ، **ثورة المعلومات وانعكاساتها على قانون العقوبات** ، ط(٢) ، القاهره: دار النهضة العربية للنشر والتوزيع

الصغير ، جميل (١٩٩٢) ، **الجرائم الناشئة عن استخدام الحاسب الآلي** ، بدون رقم طبعه ، القاهره : دار النهضة العربية.

الصغير ، جميل (٢٠٠٢)، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت** ، الطبعة (١) ، القاهره :دار النهضة العربية.

الغافري ، سعيد(٢٠٠٩) ، **السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة"**، ط(١) ، القاهره : دار النهضة العربية.

الغثبر ، خالدبن و الهيشه سليمان (٢٠٠٨) ، **الاصطياد الالكتروني : الاساليب والاجراءات المضادة** ، ط(١) الرياض : مركز التميز لأمن المعلومات

المجالي ، نظام (٢٠٠٤) ، **شرح قانون العقوبات القسم العام**،ط(١) ، عمان : دار الثقافة للنشر والتوزيع –

المناعسة ، أسامة (٢٠٠٠) ، **جرائم الحاسب الآلي والإنترنت ـ دراسة تحليلية مقارنة**، الطبعة (١) ، عمان : دار وائل للنشر .

الهريش ، فرج (١٩٩٨)، **جرائم تلويث البيئة ، دراسة مقارنة** ،ط (١) ، الرياض : المؤسسة الفنية للطباعة والنشر .

الهيتي محمد (٢٠٠٤) ، **التكنولويجا الحديثة والقانون الجنائي** ، ط (١) ، عمان : دار الثقافة

بن يونس ، عمر (٢٠٠٤) ، **الجرائم الناشئة عن استخدام الإنترنت** ، بدون طبعة ، القاهره: دار النهضة العربية

بورين ، ناتالي و جيز ، ايمانويل (٢٠٠٤م)، **اسماء مواقع الإنترنت** ، ط(١) ، لبنان : مكتبة صادر ناشرون ، لبنان .

حجازي ، عبد الفتاح (٢٠٠٧)، **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي**،ط (١) ، القاهره : دار الكتب القانونية.

حجازي ، عبد الفتاح (٢٠٠٢)، **النظام القانوني لحماية التجارة الالكترونية**، ط (١) ، الاسكندريه : دار الفكر الجامعي .

حسني ، محمود (١٩٨٤) ، **جرائم الاعتداء على الأموال في قانون العقوبات اللبناني ، دراسه مقارنه**، بدون طبعه ، بيروت. : دار النهضة العربية

حسني محمود (١٩٨٩) ، **شرح قانون العقوبات ـ القسم العام**، ، ط(٦) ، القاهره : دار النهضة العربية للنشر والتوزيع .

خليفه ، محمد (٢٠٠٧)،الحماية الجنائية لمعطيات الحاسوب الالي ، ط(١) ، الاسكندريه : دار الجامعة الجديدة

خليل ، احمد (١٩٨٢)، **مشروعية الدليل في المواد الجنائية** ، بدون رقم طبعه ، عين شمس : كلية الحقوق -جامعة عين شمس

داود ، حسن (٢٠٠٤) ، **امن شبكات الحاسوب** ، بدون رقم طبعه ، الرياض : مكتبة الملك فهد الوطنية .

رستم ، هشام (١٩٩٤) ، **الجوانب الإجرائية للجرائم المعلوماتية**، بدون طبعه ، اسيوط : مكتبة الآلات الحديثة

رستم ، هشام (١٩٩٢) ، **قانون العقوبات ومخاطر تقنية المعلومات**، الطبعة الأولى، اسيوط : مكتبة الآلات الحديثه

رمضان ، عمر (١٩٩٨) ، **شرح قانون العقوبات القسم العام** ، ط (١) ، القاهره : دار النهضة العربية ـ

سالم ، شوقى (٢٠٠١) . **نظم المعلومات والحاسب الآلى** . بدون رقم طبعه ، الإسكندرية : مركز الاسكندرية للوثائق الثقافية والمكتبات .

سرور ، أحمد (١٩٩١)، **الوسيط في قانون العقوبات - القسم العام،** الطبعة(٥) ، القاهره : دار النهضة العربية

سويلم محمد (٢٠٠١) ، **مدخل الى علم الحاسب** ، بدون طبعه، القاهره : المكتبة الأكاديمية

طلبه ، محمد (١٩٩٢) ، **فيروسات ا لحاسب وأمن البيانات** ، ط(١) ، القاهره :مطابع الكتاب المصري

عبد الستار ، فوزية(١٩٩٢) ، **شرح قانون العقوبات - القسم العام،** بدون ذكر رقم الطبعة، القاهره : دار النهضة العربية

عبد القوي ، عبد الصبور(٢٠١٠) ، **الجريمة الالكترونية** ،ط (١)، القاهره: دار العلوم للنشر والتوزيع .

عبد المنعم ، سليمان(١٩٩٨) ، **النظرية العامة لقانون العقوبات** ،ط (١) الاسكندريه : دار الجامعة الجديدة للنشر .

عرب ، يونس (٢٠٠١) ، **موسوعة القانون وتقنية المعلومات** ، ط١ ،بيروت : منشورات اتحاد المصارف العربية .

عيسى ، طوني (٢٠٠١) ، **التنظيم القانوني لشبكة الانترنت (دراسة مقارنة)** ، ط(١) ، بيروت : دار صادر ناشرون –لبنان.

قاسم ، حشمت (١٩٩١) ، **علم المعلومات بين النظرية والتطبيق** ، بدون رقم طبعه، القاهره : مكتبة غريب .

قشقوش ، هدى (١٩٩٢) ، **جرائم الحاسب الالكتروني في التشريع المقارن،** ط(١) ، القاهره : دار النهضة العربية للنشر والتوزيع .

قشقوش ، هدى (٢٠٠٠) ، **الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت** ، ط(١) ، القاهره: دار النهضة العربية للنشر والتوزيع

قورة ، نائلة (٢٠٠٥) ، **جرائم الحاسب الآلي دراسة نظرية تطبيقية،** ط(١) ، بيروت : منشورات الحلبي

قوره ، نائله (٢٠٠٤) ، **جرائم الحاسب الاقتصادية** ، ط(١) ، القاهره : دار النهضة العربية للنشر والتوزيع .

محب الدين ، محمد (١٩٩٥) ، **البيئة في القانون الجنائي** ،ط(١) ، القاهره: مكتبة الانجلو مصريه .

مراد ،عبد الفتاح (١٩٩٠) ،مراد شرح **جرائم الكمبيوتر والانترنت،** الناشر : المؤلف نفسه ، الهيئة القومية لدار الكتب والوثائق المصرية

مصطفى ، محمود (١٩٧٤) ، **شرح قانون العقوبات القسم العام** ، بدون طبعه القاهره: دار النهضة العربية للنشر والتوزيع .

ممدوح ، خالد (٢٠٠٩) ، **فن التحقيق الجنائي في الجرائم الإلكترونية** ، ط(١) ، الاسكندريه : دار الفكر الجامعي .

ناعسه ، مروان (١٩٩٧) ،**مبادئ الحاسوب و البرمجة بلغة بيسك** ،ط (١)، عمان : دار المسيرة عمان.

هنداوي ، نور الدين (١٩٨٥) ، **الحماية الجنائية للبيئة ، دراسة مقارنة** ، ط(١) ، القاهره : دار النهضة العربية للنشر والتوزيع .

الرسائل الجامعية والأبحاث والمقالات

أبو الوفا محمد أبو الوفا **المواجهة الاجرائية للجرائم المعلوماتية** بحث مقدم من أ.د في ندوة عقدت بجامعة الامارات–العين بتاريخ ٢٠١٠/١١/٢٤ تحت عنوان **مكافحة جرائم تقنية المعلومات**

أمجد حسان **الفيروسات إرهاباً تهدد أنظمة المعلومات** ، مقال مقدم من إلى مؤتمر " **الإرهاب في عصر الرقمي**" "الذي عقد في جامعة الحسين بن طلال معان –الاردن"٢٠٠٨/٧/١٢–

حسين بن سعيد الغافري،ورقة بحثيه بعنوان **الجوانب القانونية للمعلوماتية بين النظرية والتطبيق،** مقدمة في المؤتمر العلمي الاول ا في جامعة السلطان قابوس في الفترة في الفترة من ١٣ – ٢٠١١/٣/١٤ م

حسين بن سعيد الغافري ، **الجرائم الافتراضية وجهود سلطنة عمان التشريعية في مواجهتها** ورقة عمل قدمت في المؤتمر العلمي الأول " **الجوانب القانونية للمعلوماتية بين النظرية والتطبيق** " كلية الحقوق – جامعة السلطان قابوس في الفترة من ١٣ – ٢٠١١/٣/١٤ م

ذياب البداينة ، **المنظور الاقتصادي والتقني والجريمة المنظمة** ، ضمن أبحاث حلقة علمية حول **الجريمة المنظمة وأساليب مكافحتها** ، التي نظمتها **أكاديمية نايف العربية للعلوم الأمنية** ، ١٤ ــ ١٨ نوفمبر ١٩٩٨ ، مركز الدراسات والبحوث ــ الرياض ، ١٩٩٩ ، ص٢٠٩ وما بعدها

رائد بلاسمه "**جرائم الحاسوب**"، ورقة مقدمة من قبل النقيب **الى مؤتمر الامن والسلامة المعلوماتية** الذي عقد في الجامعه الاردنية في الفترة من ٢١–٢٠١١/١١/٢٣

راشد بن حمد البلوشي ورقه عمل حول **الدليل في الجريمة المعلوماتية** مقدمه الي المؤتمر الدولي الاول حول **حماية امن المعلومات و الخصوصيه** في قانون الانترنت" الفتره من ٢ الى ٤ يونيو ٢٠٠٨القاهرة جمهورية مصر العربية

زكي أمين حسونة، **جرائم الكمبيوتر والجرائم الأخرى في مجال** التكنيك المعلوماتي. بحث مقدم للمؤتمر السادس (. للجمعية المصرية للقانون الجنائي. القاهرة، ١٩٩٣

سامي الشوا، **الغش المعلوماتي كظاهرة اجرامية مستحدثة**، ورقة عمل مقدمة **للمؤتمر السادس للجمعية المصرية للقانون الجنائي**، القاهرة، ٢٥–٢٨ تشرين أول / أكتوبر ١٩٩٣

سامي حمدان الرواشده/د.أحمد موسى الهياجنه، **مكافحة الجريمة المعلوماتية بالتجريم والعقاب : القانون الانجليزي نموذجا**، بحث محكم منشور في المجلة الاردنية في **القانون والعلوم السياسية** ، المجلد(١) العدد(٣) تشرين الاول ٢٠٠٩

شريف محمد غنام، **حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، مجلة الحقوق – جامعة الكويت**، العدد الثالث السنة ٢٨، سبتمبر

صالح أحمد البربري ، **دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية** الموقعة في بودابست ٢٠٠١/١١/٢٣ صفحه١

عارف خليل أبو عيد ، بحث في **جرائم الانترنت: دراسة مقارن**، مجلة جامعة الشارقة للعلوم الشرعية والقانونية المجلد٥، العدد ٣ ، صفحه ٣

عاصم علي الجدوع "**تحديات السلامة المعلوماتية وحما ية الفضاء المعلوماتي والامكانات التي يتيحها الفضاء المعلوماتي الامن**"، ورقة مقدمة الى **مؤتمر الامن والسلامة المعلوماتية** الذي عقد في الجامعه الاردنية في الفترة من ٢١-٢٣/١١/٢٠١١

عبد الرحمن بن عبدالله السند : **وسائل الإرهاب الإلكتروني " حكمها في الإسلام وطرق مكافحتها**" ، بحث مقدم **للمؤتمر العالمي عن موقف الإسلام من الإرهاب** ، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية ٢٠٠٤م

عبدالله العلوي البلغيثي : "**الإجرام المعاصر ــ أسبابه وأساليب مواجهته**" ، ورقة مقدمة ضمن أشغال المناظرة الوطنية حول **(السياسة الجنائية بالمغرب : واقع وآفاق)** ، التي نظمتها وزارة العدل بمكناس خلال الفترة من ٩ ــ ١١ دجنبر (ديسمبر) ٢٠٠٤

عبد الله محمد سعيد بنمة القيري ، **الضرورية التشريعية تجاه جرائم المعلوماتية** بحث مقدم من في ندوة عقدت بجامعة الامارات–العين بتاريخ ٢٤/١١/٢٠١٠ تحت عنوان **مكافحة جرائم تقنية المعلومات**

عرشوش سفيان، **جرائم المساس بأنضمة الكمبيوتر** ، بحث تخرج ، المركز الجامعي خنشله –الجزائر ، معهد العلوم القانونية ، ٢٠٠٥/٢٠٠٦ ،

علي محمود علي حموده ، **الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي لمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ر:اكادمية شرطة دبي** ، مركز البحوث والدراسات رقم العدد : ١ السنة : ٢٠٠٣تاريخ الإنعقاد: ٢٦ نيسان ٢٠٠٣تاريخ الإنتهاء: ٢٨ نيسان ٢٠٠٣

غنام محمد غنام، **عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر**، بحث مقدم إلى **مؤتمر القانون والكمبيوتر** ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، مايو ٢٠٠٠.

فشار عطاء الله ، **مواجهة الجريمة المعلوماتية في التشريع الجزا**ئري ،بحث مقدم **إلى الملتقى المغاربى حول القانون والمعلوماتية** تم عقده بأكاديمية الدراسات العليا بليبيا فى أكتوبر ٢٠٠٩

قارة آمال(٢٠٠٢)، **الجريمة المعلوماتية** رسالة ماجستير ، جامعة الجزائر كلية الحقوق – بن عكنون

محمد أبو العلا عقيدة ، **التحقيق وجمع الادلة في مجال الجرائم الالكترونية** ، ورقة عمل قدمت في **المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية** /:اكادمية شرطة دبي ، تاريخ الإنعقاد: ٢٦ نيسان – ٢٨ نيسان ٢٠٠٣

محمد حسام محمود لطفي : **المشكلات القانونية في مجال المعلوماتية** " خواطر وتأملات" ، بحث مقدم إلى مؤتمر تحديات حماية الملكية الفكرية من منظور عربي ودولي والذي عقد في القاهرة في الفترة من ٢١-٢٣/٣/ ١٩٩٧م

محمد عبد الله المنشاوي(٢٠٠٣) ، **جرائم الانترنت في المجتمع السعودي** ، رسالة ماجستير، جامعة الملك سعود، الرياض .

محمد سامي الملا (١٩٦٩)، **اعتراف المتهم** ، رسالة دكتوراه ، جامعة القاهرة ، القاهره –مصر
مدحت رمضان ، **الحماية الجنائية لموقع الإنترنت ومحتوياته** ، ورقة عمل مقدمة لندوة التجارة الإلكترونية المنعقدة في المعهد العالي للعلوم القانونية والقضائية – بدبي ، ١٠-١١ مايو٢٠٠٤

موسى مسعود ارحومة ،**الإشكاليـــــات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية** ، ورقة عمل قدمت في المؤتمر المغاربي الاول حول المعلوماتية والقانون والذي عقد في أكاديمية الدراسات العليا ــ طرابلس خلال الفترة ٢٨ ــ ٢٩ / ١٠ / ٢٠٠٩

موسى مسعود ارحومة ، **الإرهاب والإنترنت** ، بحث مقدم **إلى المؤتمر الدولي لجامعة الحسين بن طلال بعنوان : الإرهاب في العصر الرقمي** ، المنعقد بمدينة معان ــ الأردن ، خلال الفترة ١٠ ــ ٢٠٠٨/٧/١٣ .

موسى مسعود ارحومة ، **تحديد النطاق المكاني لجرائم تلويث البيئة البحرية والقانون الواجب التطبيق ، ورقة مقدمة إلى المؤتمر العلمي الخامس لكلية الشريعة والقانون/جامعة إربد الأهلية** بعنوان : "البيئة في ضوء الشريعة والقانون ــ واقع وتطلعات" ــ الأردن ، خلال الفترة ١٢ ــ ١٣/تموز (يوليو) ٢٠٠٦

نهلا المومني (٢٠٠٥)، **الجريمة المعلوماتية في قانون العقوبات الاردني** ، رسالة ماجستير الجامعة الاردنية، عمان –الاردن

يونس عرب، **التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية** ،ورقة عمل مقدمة امام **الندورة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي – دمشق**

يونس عرب ، " **صور الجرائم الالكترونية** " ورقة عمل قدمت في ندوة " **تطوير التشريعات في مجال مكافحة الجرائم الالكترونية** " التي نظمتها هيئة تنظيم الاتصالات / مسقط – سلطنة عمان ٢-٤ ابريل ٢٠٠٦

الابحاث والمقالات المنشورة على الانترنت

أحمد فرج أحمد للدكتور أحمد فرج.، مقدمة عامة عن الحاسبات الآلية ، محاضرات منشوره على موقع بوابة الدكتور احمد فرج ٢٠١١/١١/٥
http://ahmed.farag.free.fr/documents/Cours_Informatique/Introduction_Informatique_Premier.htm

حسين سعيد/القرصنة الالكترونية
http://www.nabdh-alm3ani.net/nabdhat/t33913.html

حسين بن سعيد الغافري ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، بحث منشور على 14/11/2011**http://www.omanlegal.net/vb/showthread.php?t=376**

حسين بن سعيد بن سيف الغافري الجرائم الواقعة على التجارة الإلكترونية ، سلطنة عمان مسقط ٢٠٠٦
http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106 2011-11-12198&Type=3

.خالد عبدالله القائفي - التحقيق الجنائي الرقمي، بحث منشور على الرابط التالي:
٢٠١١/١٠/٢٥ **www.min-mag.com/researches/mindex.php**

شيماء عبد الغني محمد عطا الله مكافحة جرائم المعلوماتية في المملكة العربية السعودية بحث منشور
http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx#_ftn4: 21/11/2011

صالح أحمد البربري دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٠٠١/١١/٢٣ **www.arablawinfo.com** الدليل الإلكتروني للقانون

عبد الكريم خالد الشامي ،جرائم الكمبيوتر والانترنت في التشريع الفلسطيني ، مقال منشور في جريدة دنيا الوطن بتاريخ ٢٠١٠/٥/٢
http://pulpit.alwatanvoice.com/articles/2010/05/02/196865.html

محمد محمد الألفي : أنماط جرائم الإنترنت ، بحث منشور على شبكة الإنترنت بتاريخ ٢٠٠٥/٩/٢٤م من خلال موقع **www.eastlaws.com**

محمد نور شحاته:التجارة الإلكترونية،بحث منشور بتاريخ ٢٠٠٥/٥/١٥م على شبكة الإنترنت:
2011-11-12www.eastlaws.com

هزوان الوز، تكنولوجيا المعلومات والتجارة الإلكترونية ، مقال منشور
http://www.alazmenah.com/?page=show_det&category_id=13&id=23513

وليد الكشباطي، جرائم اختراق الأنظمة المعلوماتيّة ، بحث منشور على
٩-١١-٢٠١١ **http://www.chawkitabib.info/spip.php?article477**

وليد عاكم ، التحقيق في جرائم الحاسوب ، بحث منشور على الانترنت
٢٠١١/١٠/١٥ **http://www.wasmia.com/jazy/crime09.pdf**

ياسر شقير ، تنازع القوانين والاختصاص القضائي وفق قانون جرائم أنظمة المعلومات المؤقت ، مقاله منشوره في جريدة الدستور الاردنية على الرابط:
http://www.addustour.com/ViewTopic.aspx?ac=\LocalAndGover\2010\12\LocalAndGover_issue1170_day28_id291621.htm#.Tukcj1bpiSo

يونس عرب : الملكية الفكرية للمصنفات الرقمية ، دراسة منشورة على شبكة الإنترنت من خلال : **www.arablaw.net** ص٢

إختراق المواقع وطرق الوقاية – دراسة منشورة على شبكة الإنترنت بتاريخ ٢٠٠٥/٩/٦ من خلال موقع2011-11-12 www.websy.net/learn/hackers/course44.htm:

اختراق المواقع الالكترونية حال الأزمات: تشخيص وحلول بحث منشور على الانترنت:
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/50-internet-and-web-services-security/1192-hacking-websites-in-crisis-diagnosis-and-solutions.html ٢٠١١/١١/٤

المذكرة الايضاحية لقانون جرائم أنظمة المعلومات
http://www.slideshare.net/UrdunMubdi3/31-72010-2 18/11/2011

السمات الحيوية – البصمة الصوتية ، مقال منشور على موقع مركز التميز لامن المعلومات الرابط:
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/53-smart-card-and-biometrics-security/1495-vital-features-voice-tag.html ٢٠١١/١١/١٣

الدخول غير المشروع على انظمة انظمة المعلومات، بحث منشور على الانترنت:
http://irbd.hooxs.com/t16012-topic 17/11/2011

امن المعلومات ، مقال منشور ، تاريخ الزياره ، 15/11/2011
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar

تقنيات الأدلة الجنائية الإلكترونية ن مقال علمي للكاتبة جمانة كاظم علي الخليفة ، منشرو على الانترنت
http://coeia.edu.sa/images/stories/PDFs/techniques-of-e-forensic.pdf
٢٠١١/١٢/٣

جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بحث منشور على الانترنت
٢٠١١/١١/١٥
http://forum.kooora.com/f.aspx?t=16193884

التخلص من الإعلانات والكعكات (Cookies) والمخترقين– دراسة منشورة على شبكة الإنترنت (موقع الحماية والهاكرز) الرابط :
http://www.websy.net/learn/hackers/course46.htm ٢٠١١/١١/١٧

ماهي تقنية المعلومات ، مقال منشور ، المصدر موقع مكتوب ،
http://www.mktoob.com/vb/showthread.php?p=1579

ما هو الموقع الإلكتروني ؟ مقال منشور على موقع داتا تكنولوجي
http://kenanaonline.com/users/MST/topics/61250/posts/102134 ٢٠١١/١٠/٢٠

المختصر المفيد في تعليم مباديء الحاسب الالي ، مقال منشور على
http://adel900046.atspace.com/Division1.HTML 5/11/2011

القوانين

قانون العقوبات الاردني لعام ١٩٦٠ المنشور في الجريدة الرسمية بتاريخ ١٩٦٠/١/١
قانون جرائم أنظمة المعلومات مؤقت لعام٢٠١٠
قانون اصول المحاكمات الجزائية لعام رقم ٩ ١٩٦١
قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩
قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧
قانون المعاملات الالكترونية الاردني رقم ٨٥ سنة ٢٠٠١
قانون المعاملات والتجارة الالكترونية الاماراتي رقم ٢ لسنة ٢٠٠٢
قانون المعاملات الإلكترونية العماني رقم ٥ لسنة ٢٠٠٨
قانون الجزاء العماني رقم ٧ لسنة ١٩٧٤
قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم ٢ لسنة ٢٠٠٦
قانون العقوبات القطري رقم ١١ لسنة ٢٠٠٤

المراجع الاجنبية

1.Om forester(1989), **Essential proplems to Hig-Tech Society First MIT .**Pres edition, Cambridge, Massachusetts.

2. A. Emigh(2005)**, "Online Identity Theft**: Phishing Technology, Chokepoints and Countermeasures", Radix Labs .

3.Waslk Martin(1991). **crime and computer** ,Oxford University ,press, p136 ; Vergucht (Pascal): op. cit.

4.Conley Jonhn (1999), **A survey of computer crime legislation in United States** , I.C.T.L .

5. KEIIY Stein(2000) **,"Unauthorized Access and the Computer Misuse**: House of Lords Leaves no Room for Ambiguity" Computerand Telecommmunications Law Review .

THE CRIMINAL OFFENCE OF IIIEGAL ENTRY TO ELECTRONIC SITE OR INFORMATION SYSTEM ACCORDING TO JORDANIAN LAW – COMARATIVE STUDY

By
Mohmmad S. Al-Alkawaldeh

Supervisor
Dr. Ahmmad M. Hayajneh

ABSTRACT

Study addresses the crime of illegal entry of a website or information system in Accordance with Jordanian legislation, specifically according to the provisions contained in the Crimes Act Information Systems 2010.Where spread offenses Penetrate Many websites and unauthorized access to system information in order to capture or destruction of information-through IT viruses and Other Means of destruction.

In this study we describe the nature of legal form of illegal entry website or information system, and Analyzing the The Most Important Characteristics of this crime to Be Applied to the reality of the legal text by Describing the elements of this crime and criminal activity component Have pictures , and The Responsibility of the perpetrator of this type of crime and the penalty to Be Developed in Accordance with the text of the Jordanian law, Compared with the comparison of criminal legislation.

The study concluded a number of findings and recommendations that was the crime of illegal entry of the information system or Website crime, based on intelligence Without the Slightest effort muscle.

It is necessary to introduce legal provisions to punish the crime of destruction of the information and data Itself, In addition to the criminalization of a legal entity such as companies and agencies in the event of one of its employees to committing a crime.